ID: 1417615
Sample Name:
SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe
Cookbook: default.jbs
Time: 19:18:05
Date: 29/03/2024
Version: 40.0.0 Tourmaline

Table of Contents

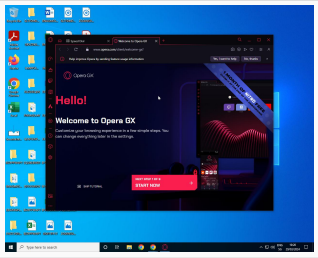
Windows Analysis Report

SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe

Overview

General Information

Sample name:	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe
Analysis ID:	1417615
MD5:	dbb69ee00786…
SHA1:	40a82d88b06e…
SHA256:	dbc32537a29f5…
Tags:	exe
Infos:	



Detection

Score:	34
Range:	0 - 100
Whitelisted:	false
Confidence:	0%

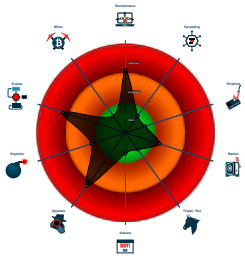
Compliance

Score:	35
Range:	0 - 100

Signatures

- Multi AV Scanner detection for subm…
- Contains functionality to register a lo…
- Found direct / indirect Syscall (likely…
- Installs a global event hook (focus c…
- Tries to harvest and steal browser in…
- Writes many files with high entropy
- Adds / modifies Windows certificates
- Binary contains a suspicious time s…
- Contains functionality for execution …
- Contains functionality to check if a d…
- Contains functionality to communica…
- Contains functionality to dynamicall…
- Contains functionality to launch a pr…

Classification



Analysis Advice

Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Sample searches for specific file, try point organization specific fake files to the analysis machine

Sample has functionality to log and monitor keystrokes, analyze it with the 'Simulates keyboard and window changes' cookbook

Process Tree

- **System is w10x64**
- SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe (PID: 6512 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe" MD5: DBB69EE00786BED3E12A04518E0F469A)
  - SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp (PID: 5996 cmdline: "C:\Users\user\AppData\Local\Temp\is-TG3DC.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp" /SL5="$1043A,1055917,832512,C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe" MD5: 668D5368DEF8B65631C43EECBD50EA48)
    - OperaGXSetup.exe (PID: 1396 cmdline: "C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe" --silent --allusers=0 MD5: 3C5239C753641E08EA3C2080FBFD5D51)
      - OperaGXSetup.exe (PID: 3276 cmdline: C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win32 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x2e4,0x2e8,0x2ec,0x2c0,0x2f0,0x6bb4623c,0x6bb46248,0x6bb46254 MD5: 3C5239C753641E08EA3C2080FBFD5D51)
      - OperaGXSetup.exe (PID: 5068 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\OperaGXSetup.exe" --version MD5: 3C5239C753641E08EA3C2080FBFD5D51)
      - OperaGXSetup.exe (PID: 652 cmdline: "C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe" --backend --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --consent-given=0 --general-interests=0 --general-location=0 --personalized-content=0 --personalized-ads=0 --launchopera=1 --installfolder="C:\Users\user\AppData\Local\Programs\Opera GX" --profile-folder --language=en-GB --singleprofile=0 --copyonly=0 --allusers=0 --setdefaultbrowser=1 --pintotaskbar=1 --pintostartmenu=1 --run-at-startup=1 --server-tracking-data=server_tracking_data --initial-pid=1396 --package-dir-prefix="C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_20240329191858" --session-guid=8ddbc8bc-ca9a-4c2b-a001-468713504759 --server-tracking-blob=NGFjMjBjZGM2OTE2N2RiNmJlYjJmY2M2YTBmZDdmMDY4ZjE3N2Y3OWFjNmExN2RhOTU2NGUyNWUyOTFkYjhlNjp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4dln0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21lZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04MDVjOTQ2ZWM3YzU0NjgwYjM3ZjU4MmQ1OGRlMTgzMCZ1dG1fY29udGVudD0zNzQyX3NldHVwaW8iLCJzeXN0ZW0iOnsicGxhdGZvcm0iOnsiYXJjaCI6Ing4NI82NCIsIm9wc3lzIjoiV2l

uZG93cyIsIm9wc3lzLXZlcnNpb24iOiIxMCIsInBhY2thZ2UiOiJFWEUifX0sInRpbWVzdGFtcCI6IjE3MTE3MzYzMzYuNTM0NCIsInVzZXJhZ2VudCI6IklubmF8gU2V0dXAgNi4yLjIiLCJ1dG0iOnsiY2FtcGFpZ24iOiJQV05fVVNfUEI0XzM3NDIiLCJjb250ZW50IjoiMzc0Ml9zZXR1cGlvIiwiaWQiOiI4MDVjOTQ2ZWM3YzU0NjgwYjM3ZjU4MmQ1OGRlMTgzMCIsIm1lZGl1bSI6InBhIiwic291cmNlIjoiUFdOZ2FtZXMifSwidXVpZCI6ImFiN2E4MGUwLWY1MjItNDZjMy1iYzdlLWQxNzkzYjIwNDhlMiJ9 --silent --desktopshortcut=1 --wait-for-package --initial-proc-handle=7005000000000000 MD5: 3C5239C753641E08EA3C2080FBFD5D51)

- OperaGXSetup.exe (PID: 4612 cmdline: C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win32 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x308,0x30c,0x310,0x2d8,0x314,0x6aeb623c,0x6aeb6248,0x6aeb6254 MD5: 3C5239C753641E08EA3C2080FBFD5D51)
- installer.exe (PID: 3504 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe" --backend --initial-pid=1396 --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --consent-given=0 --general-interests=0 --general-location=0 --personalized-content=0 --personalized-ads=0 --launchopera=1 --installfolder="C:\Users\user\AppData\Local\Programs\Opera GX" --profile-folder --language=en-GB --singleprofile=0 --copyonly=0 --allusers=0 --setdefaultbrowser=1 --pintotaskbar=1 --pintostartmenu=1 --run-at-startup=1 --server-tracking-data=server_tracking_data --package-dir="C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581" --session-guid=8ddbc8bc-ca9a-4c2b-a001-468713504759 --server-tracking-blob=NGFjMjBjZGM2OTE2N2RiNmJlYjJmY2M2YTBmZDdmMDY4ZjE3N2Y3OWFjNmExN2RhOTU2NGUyNWUyOTFkYjhlNjp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21lZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04MDVjOTQ2ZWM3YzU0NjgwYjM3ZjU4MmQ1OGRlMTgzMCIsIm1lZGl1bSI6InBhIiwic291cmNlIjoiUFdOZ2FtZXMifSwidXVpZCI6ImFiN2E4MGUwLWY1MjItNDZjMy1iYzdlLWQxNzkzYjIwNDhlMiJ9 --silent --desktopshortcut=1 --install-subfolder=107.0.5045.79 MD5: 21AD4599ABD2E158DB5128F32D3CC4EE)
  - installer.exe (PID: 6188 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x2c8,0x2cc,0x2d0,0x2a4,0x2d4,0x7ff8a8dad180,0x7ff8a8dad18c,0x7ff8a8dad198 MD5: 21AD4599ABD2E158DB5128F32D3CC4EE)
  - explorer.exe (PID: 1028 cmdline: C:\Windows\Explorer.EXE MD5: 662F4F92FDE3557E86D110526BB578D5)
    - opera.exe (PID: 5144 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --start-maximized --ran-launcher --instance-name=a7abe095bcfd6dc868442c2e858a30d1 --splash-handle=1040 --lowered-browser MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera_crashreporter.exe (PID: 2436 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_crashreporter.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x290,0x294,0x298,0x28c,0x29c,0x7ff8a6189628,0x7ff8a6189638,0x7ff8a6189648 MD5: 26DF88B2E68E23B60C0EEAB3E29496BB)
      - opera.exe (PID: 2952 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=gpu-process --no-appcompat-clear --start-stack-profiler --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAAAB gAAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAgAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=1848 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:2 MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera.exe (PID: 5436 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --enable-quic --no-appcompat-clear --start-stack-profiler --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=1972 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8 MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera.exe (PID: 3136 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=2776 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8 MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera.exe (PID: 5372 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=3216 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8 MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera.exe (PID: 3204 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=3356 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8 MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera.exe (PID: 5336 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=4364 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8 MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera.exe (PID: 6452 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=4764 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8 MD5: F452A15BC7E4392149F6BB2675EAAA59)
    - launcher.exe (PID: 5656 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe" --start-maximized MD5: D737A64C835D918DBE53B2C7724488FF)
      - opera_gx_splash.exe (PID: 2992 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_gx_splash.exe" --instance-name=a7abe095bcfd6dc868442c2e858a30d1 MD5: 706FE814240C22A6CB09FBF48CB86020)
      - opera.exe (PID: 3656 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --start-maximized --ran-launcher --instance-name=a7abe095bcfd6dc868442c2e858a30d1 --splash-handle=1040 MD5: F452A15BC7E4392149F6BB2675EAAA59)
        - opera_crashreporter.exe (PID: 5860 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_crashreporter.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x284,0x288,0x28c,0x280,0x290,0x7ff8a6189628,0x7ff8a6189638,0x7ff8a6189648 MD5: 26DF88B2E68E23B60C0EEAB3E29496BB)
    - koksDTqWjvmuJdFhyPGiECl.exe (PID: 6416 cmdline: "C:\Program Files (x86)\iVbaHhMGgjRPQdstHmqQTgkbxiYBLxBpyzsEuAKAsKqyZeBOViMTYbkOnfuIVKzSyxpCQrvLHujso\koksDTqWjvmuJdFhyPGiECl.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
    - koksDTqWjvmuJdFhyPGiECl.exe (PID: 1096 cmdline: "C:\Program Files (x86)\iVbaHhMGgjRPQdstHmqQTgkbxiYBLxBpyzsEuAKAsKqyZeBOViMTYbkOnfuIVKzSyxpCQrvLHujso\koksDTqWjvmuJdFhyPGiECl.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
- Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe (PID: 4952 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe" MD5: E9A2209B61F4BE34F25069A6E54AFFEA)
- assistant_installer.exe (PID: 4320 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe" --version MD5: 4C8FBED0044DA34AD25F781C3D117A66)
  - assistant_installer.exe (PID: 2964 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assis

tant\assistant_installer.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win32 --annotation=prod=OperaDesktopGX --annotation=ver=73.0.3856.382 --initial-client-data=0x270,0x274,0x278,0x24c,0x27c,0xdb4f48,0xdb4f58,0xdb4f64 MD5: 4C8FBED0044DA34AD25F781C3D117A66)

- launcher.exe (PID: 1220 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe" --scheduledautoupdate 0 MD5: D737A64C835D918DBE53B2C7724488FF)
  - installer.exe (PID: 2316 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\0EA40E5AB06B\installer.exe" --version MD5: 21AD4599ABD2E158DB5128F32D3CC4EE)
  - opera_autoupdate.exe (PID: 5516 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe" --pipeid=oauc_task_piped42b87436846297e467003cba27fe2f4 --version=107.0.5045.79 --producttype --requesttype=automatic --downloaddir="C:\Users\user\AppData\Local\Temp\.opera\0EA40E5AB06B" --installationdatadir="C:\Users\user\AppData\Local\Programs\Opera GX" --operadir="C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79" --installdir="C:\Users\user\AppData\Local\Programs\Opera GX" --user-data-dir="C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable" --nometrics --scheduledtask MD5: 6026F4719045033EFD7EC6127ED6370C)
    - opera_autoupdate.exe (PID: 2972 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe" --type=crashpad-handler "--user-data-dir=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x22c,0x230,0x234,0x208,0x238,0x7ff6e85938fc,0x7ff6e8593908,0x7ff6e8593918 MD5: 6026F4719045033EFD7EC6127ED6370C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Compliance

EXE planting / hijacking vulnerabilities found
Uses 32bit PE files
Creates a software uninstall entry
Creates install or setup log file
Creates license or readme file
PE / OLE file has a valid certificate
Contains modern PE file flags such as dynamic base (ASLR) or NX
Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to register a low level keyboard hook

Installs a global event hook (focus changed)

Spam, unwanted Advertisements and Ransom Demands

Writes many files with high entropy

HIPS / PFW / Operating System Protection Evasion

Found direct / indirect Syscall (likely to bypass EDR)

Stealing of Sensitive Information

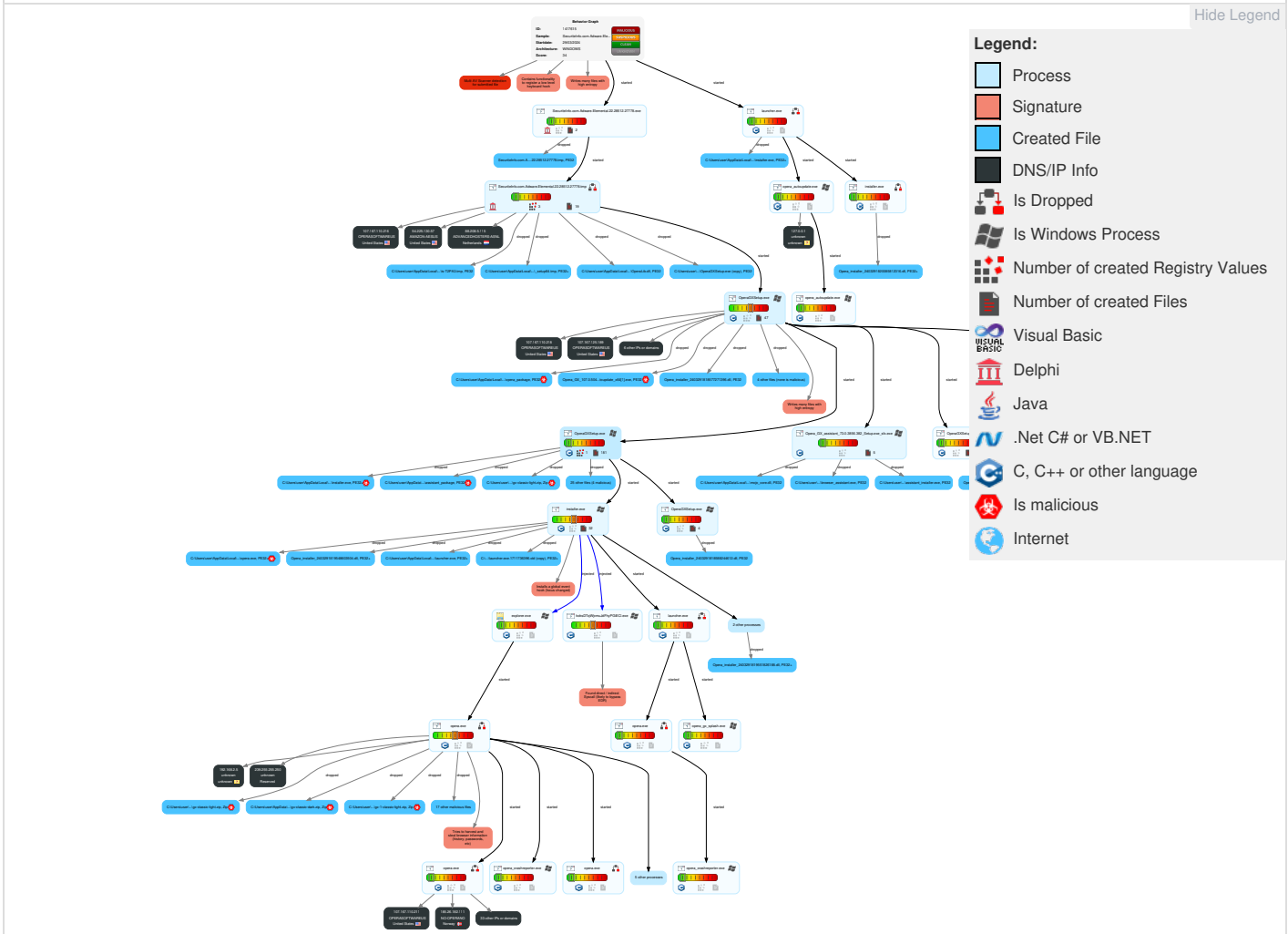
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	1 Valid Accounts	3 1 Windows Management Instrumentation	1 DLL Side-Loading	1 Abuse Elevation Control Mechanism	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	2 Native API	1 DLL Search Order Hijacking	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	1 Account Discovery	Remote Desktop Protocol	1 Browser Session Hijacking	Junk Data	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	1 2 Command and Scripting Interpreter	1 Valid Accounts	1 DLL Search Order Hijacking	1 Abuse Elevation Control Mechanism	1 1 Input Capture	4 File and Directory Discovery	SMB/Windows Admin Shares	1 Data from Local System	Steganography	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	1 Windows Service	1 Valid Accounts	3 1 Obfuscated Files or Information	NTDS	7 7 System Information Discovery	Distributed Component Object Model	1 Credential API Hooking	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	1 1 Access Token Manipulation	1 Software Packing	LSA Secrets	1 Query Registry	SSH	1 1 Input Capture	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	1 Windows Service	1 Timestomp	Cached Domain Credentials	4 1 Security Software Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	1 3 Process Injection	1 DLL Side-Loading	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 DLL Search Order Hijacking	Proc Filesystem	4 1 Virtualization/Sandbox Evasion	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 1 Masquerading	/etc/passwd and /etc/shadow	3 System Owner/User Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	1 Valid Accounts	Network Sniffing	1 Remote System Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement
Network Security Appliances	Domains	Compromise Software Dependencies and Development Tools	AppleScript	Launchd	Launchd	1 Modify Registry	Input Capture	System Network Connections Discovery	Software Deployment Tools	Remote Data Staging	Mail Protocols	Exfiltration Over Unencrypted Non-C2 Protocol	Firmware Corruption
Gather Victim Org Information	DNS Server	Compromise Software Supply Chain	Windows Command Shell	Scheduled Task	Scheduled Task	4 1 Virtualization/Sandbox Evasion	Keylogging	Process Discovery	Taint Shared Content	Screen Capture	DNS	Exfiltration Over Physical Medium	Resource Hijacking
Determine Physical Locations	Virtual Private Server	Compromise Hardware Supply Chain	Unix Shell	Systemd Timers	Systemd Timers	1 1 Access Token Manipulation	GUI Input Capture	Permission Groups Discovery	Replication Through Removable Media	Email Collection	Proxy	Exfiltration over USB	Network Denial of Service
Business Relationships	Server	Trusted Relationship	Visual Basic	Container Orchestration Job	Container Orchestration Job	1 3 Process Injection	Web Portal Capture	Local Groups	Component Object Model and Distributed COM	Local Email Collection	Internal Proxy	Commonly Used Port	Direct Network Flood

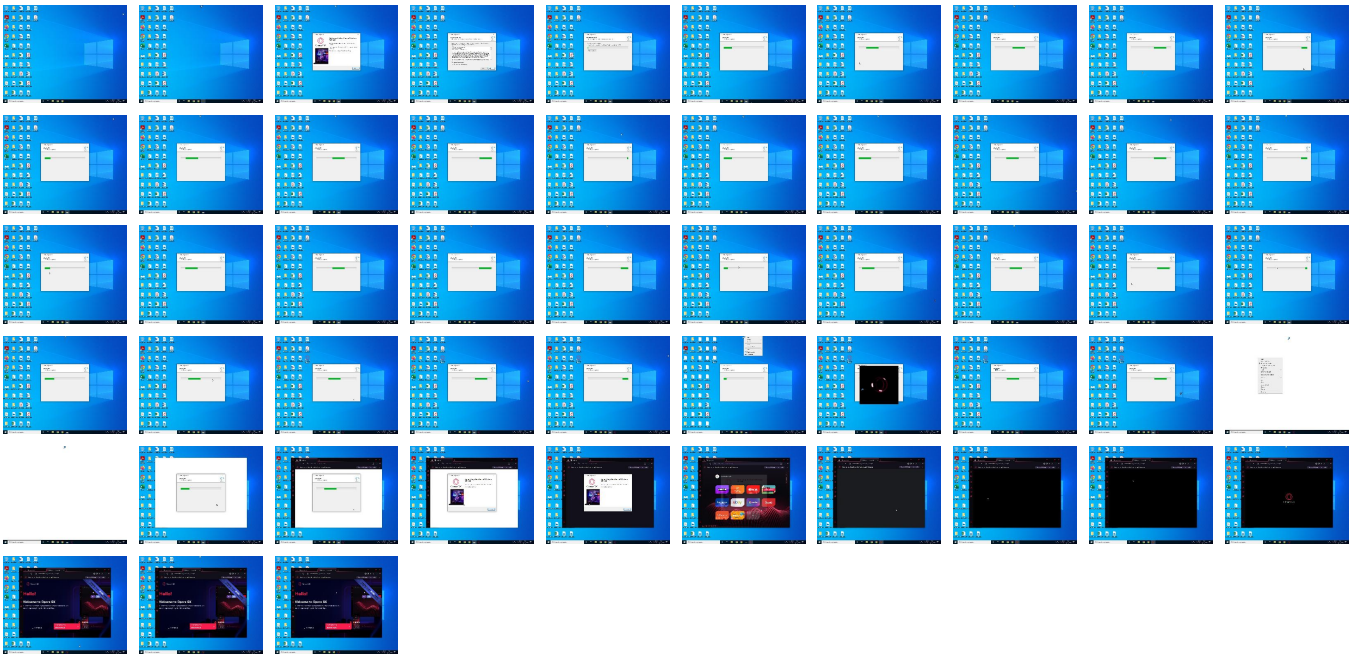
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	37%	ReversingLabs	Win32.Trojan.Generic	
SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	43%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\53IVYM2Y\Opera_GX_assistant_73.0.3856.382_Setup[1].exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\53IVYM2Y\Opera_GX_assistant_73.0.3856.382_Setup[1].exe	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9C680Q69\Opera_GX_107.0.5045.79_Autoupdate_x64[1].exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\CUESDK.x64_2017.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\CUESDK.x64_2017.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\assistant_package	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\assistant_package	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\d3dcompiler_47.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\d3dcompiler_47.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxcompiler.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxcompiler.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxil.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxil.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer_helper_64.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer_helper_64.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe.1711736396.old (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe.1711736396.old (copy)	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\libEGL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\libEGL.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\libGLESv2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\libGLESv2.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\mojo_core.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\mojo_core.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\notification_helper.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\notification_helper.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://try.opera.com/72TR8R7/KLRL579/?sub1=setupio&sub2=31120	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2008449429.0000000000993000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000011.00000000.2701335122.0000000001731000.00000002.00000001.00040000.00000000.sdmp	false		
http://https://yandex.ua/search/?clid=2358536&text=	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://legal.opera.com/terms	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2008449429.0000000000993000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000002.2850171237.000000000018A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000004.00000002.2885993218.000000000018A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000005.00000002.2061459211.00000000009CA000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000006.00000002.2922787938.000000000018A000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		
http://https://www.deezer.com/sr/login	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://api.browser.yandex.ua/suggest/get?part=	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://help.opera.com/latest/	OperaGXSetup.exe, OperaGXSetup.exe, 00000006.00000002.2922787938.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, launcher.exe, 00000012.00000002.2766223989.000060EC00288000.00000004.00001000.00020000.00000000.sdmp, opera.exe, 00000015.00000002.2787646170.0000608400254000.00000004.00001000.00020000.00000000.sdmp	false		
http://anglebug.com/4633	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/13655f413caacdcc677b24dc0c615d1f5328d6a3/	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://anglebug.com/7382	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://issuetracker.google.com/284462263	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://policies.google.com/terms;	OperaGXSetup.exe, 00000003.00000002.2850171237.000000000018A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000004.00000002.2885993218.0000000000018A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000005.00000002.2061459211.00000000009CA000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000006.00000002.2922787938.000000000018A000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		
http://https://www.baidu.com/favicon.ico	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryera.software3	OperaGXSetup.exe, 00000003.00000003.2329742679.0000000000C94000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000002.2869606187.000000000C94000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2841379432.0000000000C89000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2843461930.0000000000C93000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://ff.search.yahoo.com/gossip?output=fxjson&command=	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://autoupdate-staging.services.ams.osa/	OperaGXSetup.exe	false		
http://localhost:3001api/prefs/?product=$1&version=$2..	OperaGXSetup.exe, 00000003.00000002.2850171237.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000004.00000002.2885993218.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000005.00000002.2061459211.00000000009F0000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000006.00000002.2922787938.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		
http://www.opera.com	OperaGXSetup.exe, 00000003.00000003.2845554919.0000000036474000.00000004.00001000.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2258300885.000000003634C000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://crashpad.chromium.org/https://crashpad.chromium.org/bug/new	OperaGXSetup.exe, 00000003.00000002.2850171237.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000004.00000002.2885993218.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000005.00000002.2061459211.00000000009F0000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000006.00000002.2922787938.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe, 00000009.00000003.2278137134.00000000032A8000.00000004.00000020.00020000.00000000.sdmp, Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe, 00000009.00000003.2278137134.00000000003415000.00000004.00000020.00020000.00000000.sdmp, assistant_installer.exe, 0000000A.00000000.2279825246.0000000000D67000.00000002.00000001.01000000.00000011.sdmp, assistant_installer.exe, 0000000B.00000000.2284793354.0000000000D67000.00000002.00000001.01000000.00000011.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://desktop-netinstaller-sub.osp.opera.software/SysWOW64	OperaGXSetup.exe, 00000003.00000002.2866378247.0000000000C51000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://features.opera-api2.com/C	OperaGXSetup.exe, 00000003.00000003.2071654247.0000000000C74000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/0239ef3d7c95570d61b12b2fb509af435ccc2131/	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://www.deezer.com/no/login	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://www.deezer.com/ro/login	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://completion.amazon.com/search/complete?q=	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://anglebug.com/7714	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://listen.tidal.com/	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryera.software	OperaGXSetup.exe, 00000003.00000002.2869606187.0000000000C94000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2841379432.0000000000C89000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2843461930.0000000000C93000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/ad5beaae2fc679ccba1db1f7b3c9503d8da6ec70/	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://www.remobjects.com/ps	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1960705178.0000000002680000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1961058453.000000007FB40000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000000.1962311586.0000000000401000.00000020.00000001.01000000.00000004.sdmp	false		
http://https://www.innosetup.com/	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1960705178.0000000002680000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1961058453.000000007FB40000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000000.1962311586.0000000000401000.00000020.00000001.01000000.00000004.sdmp	false		
http://anglebug.com/6248	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://download.opera.com/R	OperaGXSetup.exe, 00000003.00000003.2090712500.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2182012704.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2087362255.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://www.deezer.com/fi/login	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://download3.operacdn.com/	OperaGXSetup.exe, 00000003.00000002.2866378247.0000000000C25000.00000004.00000020.00020000.00000000.sdmp	false		
http://anglebug.com/6929	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://anglebug.com/5281	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl4.dig-	OperaGXSetup.exe, 00000003.00000002.2870614189.0000000001068000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://www.so.com/favicon.ico	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://download5.operacdn.com/ftp/pub/opera_gx/107.0.5045.79/win/Opera_GX_107.0.5045.79_Autoupdate_	OperaGXSetup.exe, 00000003.00000003.2090712500.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000002.2866378247.0000000000C51000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2182012704.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2087414766.0000000000C8D000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2087362255.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2090712500.0000000000C8D000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2087266746.00000000041EF000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://www.deezer.com/mx/login	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://issuetracker.google.com/255411748	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000011.00000000.2719335016.000000000C8B4000.00000004.00000001.00020000.00000000.sdmp	false		
http://https://crashpad.chromium.org/	assistant_installer.exe, assistant_installer.exe, 0000000B.00000000.2284793354.0000000000D67000.00000002.00000001.01000000.00000011.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		
http://https://addons.opera.com/en/extensions/details/dify-cashback/	launcher.exe, 00000013.00000000.2728056334.00007FF7385C4000.00000002.00000001.01000000.00000017.sdmp	false		
http://https://anglebug.com/7246	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://anglebug.com/7369	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://www.deezer.com	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://anglebug.com/7489	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://autoupdate.geo.opera.com/geolocation/	OperaGXSetup.exe, OperaGXSetup.exe, 00000006.00000002.2922787938.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/appxBundleSipPutSignedDataMsgniuid=Dll-f522-46c3	OperaGXSetup.exe, 00000003.00000002.2866378247.0000000000C51000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/Xw	OperaGXSetup.exe, 00000003.00000002.2866378247.0000000000C25000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://duckduckgo.com/?q=	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://yandex.com.tr/search/?clid=1669559&text=	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		

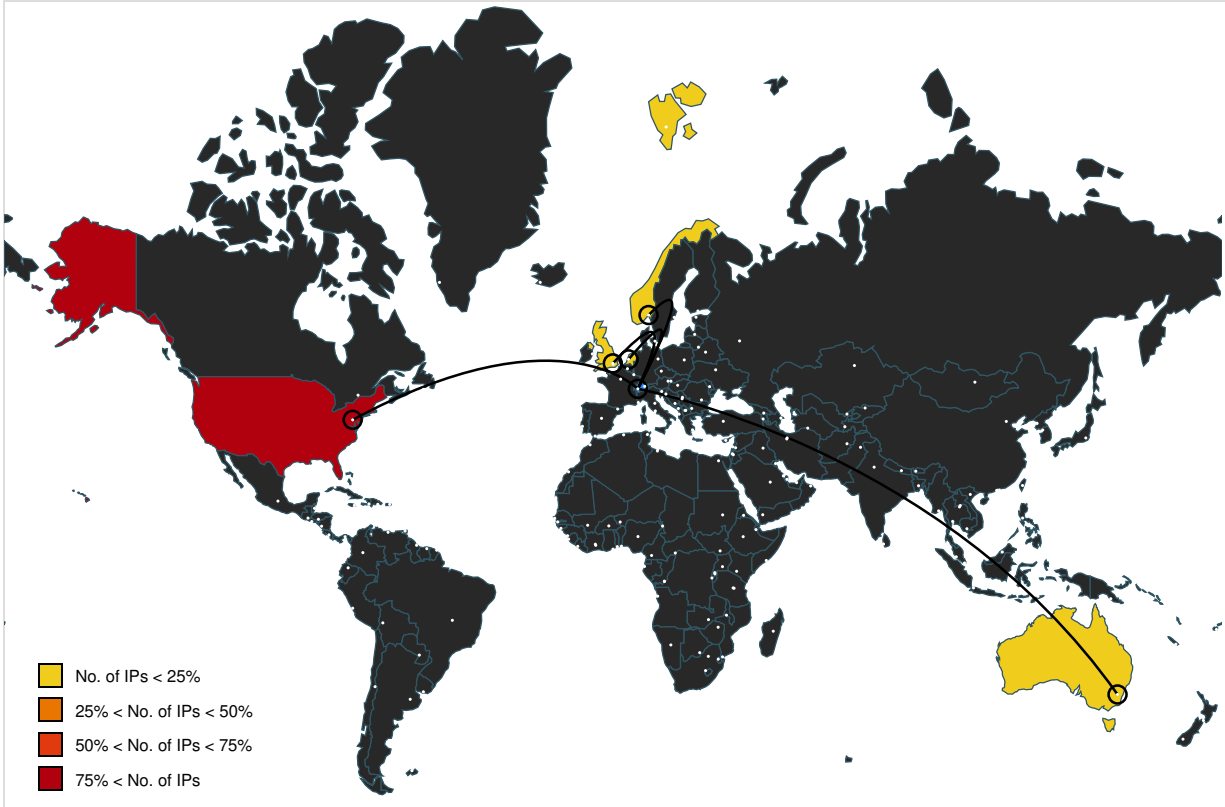
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://crashstats-collector.opera.com/collector/submit	installer.exe, 0000000E.00000002.2921864598.000001D74CF70000.00000004.00000020.00020000.00000000.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000003.2919717296.00004A5000238000.00000004.00001000.00020000.00000000.sdmp, opera.exe, 00000015.00000003.2747900384.00006084002E0000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://download.opera.com/4	OperaGXSetup.exe, 00000003.00000003.2322528834.0000000000C89000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2329742679.0000000000C94000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2090712500.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2182012704.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000002.2869606187.0000000000C94000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2841379432.0000000000C89000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2087362255.0000000000CB1000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2843461930.0000000000C93000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2258071768.0000000000C91000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2322594580.0000000000C93000.00000004.00000020.00020000.00000000.sdmp	false		
http://www.kymoto.orgAbout	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1959440394.0000000002540000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.1964992515.00000000035E0000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://try.opera.com/72TR	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2008449429.0000000000993000.00000004.00000020.00020000.00000000.sdmp	false		
http://anglebug.com/8417	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/4d3d8f7f070d279fbe0d2795e10e69fbab5d3824/	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://opera.com/privacy	OperaGXSetup.exe, OperaGXSetup.exe, 00000006.00000002.2922787938.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		
http://www.kymoto.org	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1959440394.0000000002540000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.1964992515.00000000035E0000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://issuetracker.google.com/161903006	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://www.opera.com/eula/computers	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2008449429.0000000000993000.00000004.00000020.00020000.00000000.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/etUrlCache	OperaGXSetup.exe, 00000003.00000002.2866378247.0000000000C51000.00000004.00000020.00020000.00000000.sdmp	false		

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gamemaker.io)	OperaGXSetup.exe, OperaGXSetup.exe, 0000 0006.00000002.2922787938.000000000018A00 0.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00 007FF65F517000.00000002.00000001.0100000 0.00000012.sdmp, installer.exe, 0000000E.00000000. 2628833836.00007FF65F517000.00000002.000 00001.01000000.00000012.sdmp	false		
http://autoupdate-staging.services.ams.osa/v4/v5/netinstaller///windows/x64v2/Fetching	OperaGXSetup.exe, 00000003.00000002.2850 171237.00000000001B0000.00000040.0000000 1.01000000.00000008.sdmp, OperaGXSetup.exe, 00000004.00000002.2885993218.0000000 0001B0000.00000040.00000001.01000000.000 00008.sdmp, OperaGXSetup.exe, 00000005.0 0000002.2061459211.00000000009F0000.0000 0040.00000001.01000000.0000000B.sdmp, Op eraGXSetup.exe, 00000006.00000002.292278 7938.00000000001B0000.00000040.00000001. 01000000.00000008.sdmp, installer.exe, 0 000000D.00000000.2625540919.00007FF65F51 7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836 .00007FF65F517000.00000002.00000001.0100 0000.00000012.sdmp	false		
http://https://duckduckgo.com/favicon.ico	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://www.google.com/favicon.ico	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryera.softwarep	OperaGXSetup.exe, 00000003.00000003.2322 528834.0000000000C89000.00000004.0000002 0.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2329742679.0000000 000C94000.00000004.00000020.00020000.000 00000.sdmp, OperaGXSetup.exe, 00000003.0 0000002.2869606187.0000000000C94000.0000 0004.00000020.00020000.00000000.sdmp, Op eraGXSetup.exe, 00000003.00000003.284137 9432.0000000000C89000.00000004.00000020. 00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2843461930.000000000 0C93000.00000004.00000020.00020000.00000 000.sdmp, OperaGXSetup.exe, 00000003.000 00003.2322594580.0000000000C93000.000000 04.00000020.00020000.00000000.sdmp	false		
http://anglebug.com/3078	opera.exe, 0000001C.00000003.2793241123. 00006E54023AC000.00000004.00001000.00020 000.00000000.sdmp	false		
http://anglebug.com/7553	opera.exe, 0000001C.00000003.2793241123. 00006E54023AC000.00000004.00001000.00020 000.00000000.sdmp	false		
http://anglebug.com/5375	opera.exe, 0000001C.00000003.2793241123. 00006E54023AC000.00000004.00001000.00020 000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/3ed7347a5e10c404ea6cb96281265ff23092cf8f/	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/e27cf3ebc2172a1a7d9cb6978a031ef52ed55596/	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp, installer.exe, 0000000D.000 00003.2635441252.000001D885A3C000.000000 04.00000020.00020000.00000000.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/r-sub.osp.opera.software/N	OperaGXSetup.exe, 00000003.00000002.2866 378247.0000000000C51000.00000004.0000002 0.00020000.00000000.sdmp	false		
http://anglebug.com/5371	opera.exe, 0000001C.00000003.2793241123. 00006E54023AC000.00000004.00001000.00020 000.00000000.sdmp	false		
http://https://extension-updates.opera.com/api/omaha/update/MT6L	installer.exe, 0000000D.00000003.2708034 650.00004D5400360000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://anglebug.com/4722	opera.exe, 0000001C.00000003.2793241123. 00006E54023AC000.00000004.00001000.00020 000.00000000.sdmp	false		
http://https://www.deezer.com/ru/login	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/434b0a6daa530638a964132e86b8a01d7b39aa7c/	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gamemaker.io/en/get.	OperaGXSetup.exe, OperaGXSetup.exe, 0000 0006.00000002.2922787938.000000000018A00 0.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00 007FF65F517000.00000002.00000001.0100000 0.00000012.sdmp, installer.exe, 0000000E.00000000. 2628833836.00007FF65F517000.00000002.000 00001.01000000.00000012.sdmp	false		
http://https://addons.opera.com/extensions/download/aad01b6c6f7f2f01bea6584af044c96d8850f748/	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://crashstats-collector.opera.com/collector/submitJP	installer.exe, 0000000E.00000002.2926616 195.00004A50002C4000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://gamemaker.io	OperaGXSetup.exe, OperaGXSetup.exe, 0000 0006.00000002.2922787938.000000000018A00 0.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00 007FF65F517000.00000002.00000001.0100000 0.00000012.sdmp, installer.exe, 0000000E.00000000. 2628833836.00007FF65F517000.00000002.000 00001.01000000.00000012.sdmp	false		
http://anglebug.com/7556	opera.exe, 0000001C.00000003.2793241123. 00006E54023AC000.00000004.00001000.00020 000.00000000.sdmp	false		
http://https://autoupdate.geo.opera.com/api/prefs/?product=Opera%20GX&version=107.0.5045.79	OperaGXSetup.exe, 00000003.00000002.2876 049672.00000000041ED000.00000004.0000002 0.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2841379432.0000000 000C89000.00000004.00000020.00020000.000 00000.sdmp, OperaGXSetup.exe, 00000003.0 0000003.2329765016.00000000041EE000.0000 0004.00000020.00020000.00000000.sdmp, Op eraGXSetup.exe, 00000003.00000003.232965 3768.0000000000C89000.00000004.00000020. 00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000002.2868631396.000000000 0C89000.00000004.00000020.00020000.00000 000.sdmp	false		
http://https://addons.opera.com/extensions/download/313b7f796952f2b34bf6bce6ba10a7b51bd18913/	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryera.softwareV	OperaGXSetup.exe, 00000003.00000002.2869 606187.0000000000C94000.00000004.0000002 0.00020000.00000000.sdmp, OperaGXSetup.exe, 00000003.00000003.2841379432.0000000 000C89000.00000004.00000020.00020000.000 00000.sdmp, OperaGXSetup.exe, 00000003.0 0000003.2843461930.0000000000C93000.0000 0004.00000020.00020000.00000000.sdmp	false		
http://https://translate.yandex.net/main/v2.92.1465389915/i/favicon.ico	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://addons.opera.com/extensions/download/505f20c0ceb331ebec9f6b8d9def5e0f59be4612/	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://browser-notifications.opera.com/api/v1/	Opera_GX_assistant_73.0.3856.382_Setup.e xe_sfx.exe, 00000009.00000003.2278137134 .0000000003415000.00000004.00000020.0002 0000.00000000.sdmp	false		
http://https://www.deezer.com/us/login	installer.exe, 0000000D.00000003.2707774 182.00004D5400604000.00000004.00001000.0 0020000.00000000.sdmp	false		
http://https://smolecular.icu/tfg/?src=setupIO	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2008449429.0000000 000993000.00000004.00000020.00020000.000 00000.sdmp	false		

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://autoupdate.geo.opera.com/https://autoupdate.geo.opera.com/geolocation/OperaDesktopGXhttps://	OperaGXSetup.exe, 00000003.00000002.2850171237.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000004.00000002.2885993218.0000000001B0000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000005.00000002.2061459211.00000000009F0000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000006.00000002.2922787938.00000000001B0000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000D.00000000.2625540919.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000E.00000000.2628833836.00007FF65F517000.00000002.00000001.01000000.00000012.sdmp	false		
http://https://word.office.comon	explorer.exe, 00000011.00000000.2707241317.00000000099B0000.00000004.00000001.00020000.00000000.sdmp	false		
http://anglebug.com/6692	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://issuetracker.google.com/258207403	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://https://www.deezer.com/es/login	installer.exe, 0000000D.00000003.2707774182.00004D5400604000.00000004.00001000.00020000.00000000.sdmp	false		
http://anglebug.com/3502	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		
http://anglebug.com/3623	opera.exe, 0000001C.00000003.2793241123.00006E54023AC000.00000004.00001000.00020000.00000000.sdmp	false		

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.79.197.200	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.246.40	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
54.225.130.57	unknown	United States		14618	AMAZON-AESUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.61.11.143	unknown	United States		20940	AKAMAI-ASN1EU	false
142.251.163.188	unknown	United States		15169	GOOGLEUS	false
37.228.108.132	unknown	Norway		39832	NO-OPERANO	false
142.251.111.104	unknown	United States		15169	GOOGLEUS	false
82.145.216.15	unknown	United Kingdom		39832	NO-OPERANO	false
172.253.115.147	unknown	United States		15169	GOOGLEUS	false
20.110.205.119	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
107.167.96.30	unknown	United States		53755	IOFLOODUS	false
107.167.96.31	unknown	United States		53755	IOFLOODUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
142.250.31.138	unknown	United States		15169	GOOGLEUS	false
142.251.163.119	unknown	United States		15169	GOOGLEUS	false
172.253.63.95	unknown	United States		15169	GOOGLEUS	false
37.228.108.144	unknown	Norway		39832	NO-OPERANO	false
104.45.184.134	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
172.253.63.102	unknown	United States		15169	GOOGLEUS	false
172.253.122.94	unknown	United States		15169	GOOGLEUS	false
88.208.5.115	unknown	Netherlands		39572	ADVANCEDHOSTERS-ASNL	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
107.167.110.218	unknown	United States		21837	OPERASOFTWAREUS	false
107.167.110.216	unknown	United States		21837	OPERASOFTWAREUS	false
23.48.104.107	unknown	United States		20940	AKAMAI-ASN1EU	false
107.167.110.211	unknown	United States		21837	OPERASOFTWAREUS	false
23.61.11.162	unknown	United States		20940	AKAMAI-ASN1EU	false
104.18.7.134	unknown	United States		13335	CLOUDFLARENETUS	false
13.107.21.200	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.251.16.156	unknown	United States		15169	GOOGLEUS	false
96.6.42.17	unknown	United States		20940	AKAMAI-ASN1EU	false
104.18.8.172	unknown	United States		13335	CLOUDFLARENETUS	false
142.251.167.95	unknown	United States		15169	GOOGLEUS	false
185.26.182.111	unknown	Norway		39832	NO-OPERANO	false
104.18.10.89	unknown	United States		13335	CLOUDFLARENETUS	false
18.160.41.53	unknown	United States		3	MIT-GATEWAYSUS	false
185.26.182.112	unknown	Norway		39832	NO-OPERANO	false
172.64.162.29	unknown	United States		13335	CLOUDFLARENETUS	false
142.251.167.156	unknown	United States		15169	GOOGLEUS	false
104.18.6.134	unknown	United States		13335	CLOUDFLARENETUS	false
192.229.211.108	unknown	United States		15133	EDGECASTUS	false
3.21.115.179	unknown	United States		16509	AMAZON-02US	false
142.251.16.97	unknown	United States		15169	GOOGLEUS	false
104.78.188.21	unknown	United States		16625	AKAMAI-ASUS	false
107.167.125.189	unknown	United States		21837	OPERASOFTWAREUS	false
99.84.191.43	unknown	United States		16509	AMAZON-02US	false
23.222.79.195	unknown	United States		20940	AKAMAI-ASN1EU	false

Private

IP
192.168.2.5
127.0.0.1

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1417615

Start date and time:	2024-03-29 19:18:05 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 13m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	3
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe
Detection:	SUS
Classification:	sus34.rans.spyw.evad.winEXE@118/1236@0/49
EGA Information:	• Successful, ratio: 42.9%
HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtReadFile calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtSetValueKey calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- Skipping network analysis since amount of network traffic is too extensive

Simulations

Behavior and APIs

Time	Type	Description
19:18:50	API Interceptor	4x Sleep call for process: SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp modified
19:20:03	API Interceptor	8x Sleep call for process: explorer.exe modified
19:20:04	Task Scheduler	Run new task: Opera GX scheduled Autoupdate 1711736395 path: C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe s>--scheduledautoupdate $(Arg0)
19:20:30	API Interceptor	1x Sleep call for process: opera_autoupdate.exe modified
19:20:34	API Interceptor	1x Sleep call for process: opera.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F2E248BEDDBB2D85122423C41028BFD4

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	Certificate, Version=3
Category:	dropped
Size (bytes):	1428
Entropy (8bit):	7.688784034406474
Encrypted:	false
SSDEEP:	24:nIGWnSIGWnSGc9VIyy0KuiUQ+7n0TCDZJCCAyuIqwmCFUZnPQ1LSdT:nIL7LJSRQ+QgAyuxwfynPQmR
MD5:	78F2FCAA601F2FB4EBC937BA532E7549
SHA1:	DDFB16CD4931C973A2037D3FC83A4D7D775D05E4
SHA-256:	552F7BDCF1A7AF9E6CE672017F4F12ABF77240C78E761AC203D1D9D20AC89988
SHA-512:	BCAD73A7A5AFB7120549DD54BA1F15C551AE24C7181F008392065D1ED006E6FA4FA5A60538D52461B15A12F5292049E929CFFDE15CC400DEC9CDFCA0B36A68DD
Malicious:	false
Reputation:	unknown
Preview:	0...0..x.....W..!2.9...wu\0...*.H.....0b1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1!0...U....DigiCert Trusted Root G40...130801120000Z..38011 5120000Z0b1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1!0...U....DigiCert Trusted Root G40.."0...*.H.....0.....sh..]J<0"0i3..%..!=..Y..).=X.v..{.... 0....8..V.m...y....._..<R.R....~...W.YUr.h.p..u.js2...D.....t;mq.-... .. .c)-..^N..!a.4...^.[.....4@_.zf.w.H.fWW.TX..+.O.0.V..{]..O^.5.1..^.....@.y.x...j.8.....7...}...>..p.U.A2...s*n..| !L....u]xf.:1D.3@...ZI...g.'..O9..X..$\F.d..i.v.v=Y]Bv...izH....f.t..K...c.....:.=...E%...D.+~....am.3...K...}....!.....p,A`..c.D..vb~.....d.3....C....w.....!..T)%.I..RQGt.&..Au.z._.?..A.. [..P.1..r."..|Lu?c.!_. Qko....O..E_. .....~.&...i/..-.....B0@0...U.....0....0...U.....0...U.....q]dL..g?....O0...*.H.....a.}.I.....dh.V.w.p...J...x\.._...)V.6I]Dc.. .f.#.=y.mk.T..<.C@..P.R..;...ik.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F2E248BEDDBB2D85122423C41028BFD4

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	3.0578008846792457
Encrypted:	false
SSDEEP:	6:kK9+sNlpLDcJgjcalgRAOAUSW0PTKDXMOXISKlUp:8sNlpLYS4tWOxSW0PAMsZp
MD5:	1338251D8056D8DABCA670706A5C27A1
SHA1:	EE2200F10C47D1BC18DE6DE03BD58A6CE66952C7
SHA-256:	5D6E2BDF6A9E76A39066A379AC8825BBACE7D68438C7FA598AE7C151A8FB70BA
SHA-512:	25B3C002DE3C05CBE5FAECAD343BD4086E89AE4D7D00C2FA72D57F45754D4D556BC682959B5D914B0CB20504037C5A956AFEAF1A992425AE941739A7CC9F61A9

Malicious:	false
Reputation:	unknown
Preview:	p..... ....l....0.....(..... .....n.....h.t.t.p.:.//.c.a.c.e.r.t.s...d.i.g.i.c.e.r.t...c.o.m./.D.i.g.i.C.e.r.t.T.r.u.s.t.e.d.R.o.o.t.G.4...c.r.t...".5.a.2.8.6.4.1.7.-.5.9.4."...

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000015.db

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	107064
Entropy (8bit):	4.025348499885685
Encrypted:	false
SSDEEP:	1536:/kYGWjvoGD6WyrMhlilGEn0KFJKh1Qxhwpt:/kYGQAGD6hrMhlibKF6Qxqn
MD5:	5DCD558469E8D306BA03EABAEFE2569D
SHA1:	97D648A219D80B2E9D40ACB7CE53E7B79F611780
SHA-256:	EDC7011A8A20109D2A6350CD77B016C02D81100206EF852F362FC2D204D399FD
SHA-512:	BBEF17D987AFFBABDD0E0FDA780CB0B928152BC5C9B3360D29510C7AFC6C722E443370880E1F11D52A342CDA2FC9F6392DDFDD10FAAFD25294314AD335AE0FFB
Malicious:	false
Reputation:	unknown
Preview:	....h... ...8.....P.....Y...H...`.....(.....W.....e.n.-.C.H.;.e.n.-.G.B.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>.....a.l.f.o.n.s.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....\.1.....Microsoft.D.....M.i.c.r.o.s.o.f.t.....V.1.....Windows.@.....W.i.n.d.o.w.s.....`.1.....Start Menu..F.....S.t.a.r.t. .M.e.n.u.....(.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>.....

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	105184
Entropy (8bit):	4.0385543778533926
Encrypted:	false
SSDEEP:	768:T7l6Pzk8G975szjk02kp4nVwRNMLqKyjLzMXPyAbR1vcSYB7smwypf34xeKWohIQ:gkf7Up4nVwD+vhIizG/n/sFrK1pTdA
MD5:	AF342F6A19533FA201024892E59CD664
SHA1:	F6739C86075BBD123C80CC5E9B18C67899B03845
SHA-256:	43FB539DB0029555B202799C7848CA42978D941C86C3BD9EF33060BBA4AC86D3
SHA-512:	6456F1D06C4FEEAD79D0C381A5F12B1BB82DC278C0E1F606391FE1B317085EF002DEEE86CC075EA14AAE758E665148B6DF62F02EF986E0997BC9334AD12F5CA0
Malicious:	false
Reputation:	unknown
Preview:	....h... .....P.....Y.....`...0.....x...W.....e.n.-.C.H.;.e.n.-.G.B.....P.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>.....a.l.f.o.n.s.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....\.1.....Microsoft.D.....M.i.c.r.o.s.o.f.t.....V.1.....Windows.@.....W.i.n.d.o.w.s.....`.1.....Start Menu..F.....S.t.a.r.t. .M.e.n.u.....(.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\53IVYM2Y\Opera_GX_assistant_73.0.3856.382_Setup[1].exe

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1499104
Entropy (8bit):	7.985603261747699
Encrypted:	false
SSDEEP:	24576:4ACKcQz8HkfJ8dQnd4GrbwsgY+UfLBCQdI5f3cjCRgCPPWCUZry8k/GUrbN:5pT8HkfJ5eGrbmR0afsXCBrG
MD5:	E9A2209B61F4BE34F25069A6E54AFFEA
SHA1:	6368B0A81608C701B06B97AEFF194CE88FD0E3C0
SHA-256:	E950F17F4181009EEAFA9F5306E8A9DFD26D88CA63B1838F44FF0EFC738E7D1F
SHA-512:	59E46277CA79A43ED8B0A25B24EFF013E251A75F90587E013B9C12851E5DD7283B6172F7D48583982F6A32069457778EE440025C1C754BF7BB6CE8AE1D2C3FC5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse

Reputation:	unknown
Preview:	MZ`.....@.....`.....!..L.!Require Windows..$PE..L...'..P.....(...F.....-.....@....@.....7.....b.....H.....@..d.....text....&.....(..... ..`.rdata...5...@...6...*.....@..@.data....).....`.....@....rsrc.....h.....@..@.....U..`.A.....S3.;.VWt.f9.b.A.t...`.A.P....P.|..Y.nj'.v....u..v..=.BA..6P.....P....9^..].v8.^..3.....hhDA.P.....P.....P..pAA..E..E...;F.r.....P.J\|..Y.24..j...IAA...t$..D....3.9.H.A.t...@....9D$.t..t$.Ph.....5@.A....BA.3.....D$..`...\|$..u..@.....3.....t$..D$..t$...`.A.....t$...P.Q..%`.A...D$...V...t...P.Q...^...VW.\|$.....t...W.P.....t...P.Q..>.._^....T$..L$....f..AABBf..u..L$.3.f9.t.@f.<A.u..S.\$.V..C;^.tLW3.j.Z.....Q.....3.9F.Y~.9F.~...f..Af..G@;F.|..6....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9C680Q69\Opera_GX_107.0.5045.79_Autoupdate_x64[1].exe

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	142198520
Entropy (8bit):	**7.999995421447281**
Encrypted:	**true**
SSDEEP:	3145728:4PPyb5NN6TkxOYod/OocWSqlsw6l3iYwiA1+ulOYZ:gP4Z0/jl0vVB+usg
MD5:	E5C66BC2A10855CB4164EEF86F92FB0D
SHA1:	9453AA10DE00E311EE3415D1C07F1990FE6FB491
SHA-256:	FD238E7993A9800F8B9D5C0C0F4FB90E624823BC4A085F658F9544296A4A967D
SHA-512:	CFE5614CD7FBA269DC89A69240382B42649AA45449266447EC29E95A01C69D898F317AD75E07651BD75AB7FCF42C1E6E1731457F91A51397810744D95F1F96B9
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	unknown
Preview:	MZ`.....@.....`.....!..L.!Require Windows..$PE..L...'..P.....(...F.....-.....@....@.....z.....b.....X.y..).....@..d.....text....&.....(..... ..`.rdata...5...@...6...*.....@..@.data....).....`.....@....rsrc.....h.....@..@.....U..`.A.....S3.;.VWt.f9.b.A.t...`.A.P....P.\|..Y.nj'.v....u..v..=.BA..6P.....P....9^..].v8.^..3.....hhDA.P.....P.....P..pAA..E..E...;F.r.....P.J\|..Y.24..j...IAA...t$..D....3.9.H.A.t...@....9D$.t..t$.Ph.....5@.A....BA.3.....D$..`...\|$..u..@.....3.....t$..D$..t$...`.A.....t$...P.Q..%`.A...D$...V...t...P.Q...^...VW.\|$.....t...W.P.....t...P.Q..>.._^....T$..L$....f..AABBf..u..L$.3.f9.t.@f.<A.u..S.\$.V..C;^.tLW3.j.Z.....Q.....3.9F.Y~.9F.~...f..Af..G@;F.|..6....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\1698947853-custom_partner_content[1].json

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	Unicode text, UTF-8 text, with very long lines (1824)
Category:	dropped
Size (bytes):	1344708
Entropy (8bit):	6.081849998191263
Encrypted:	false
SSDEEP:	24576:idUTvr+x0E4H3CAHkd0OhPVVUCs4dxemFiG7V76d5vQVUCaxU:iKTHhySkuz/G65v1y
MD5:	1FB07CF2B20D516ADC1067D9C4C57BB7
SHA1:	DA0BFEB9A98B2FDAF422A1B52FFA33ECA0684EA1
SHA-256:	294592F92BDDA407A531D81D64B7D141979F7B5B052370C1041430530DB7C481
SHA-512:	F4B17E1E60281465A3288E5BDE7C537AC419236A72B680AD533E93CAE81DC8E12221339A737C27257B0A561192F655C70230D818EB0219CCB5E4641B5FF811D8
Malicious:	false
Reputation:	unknown
Preview:	// DUwgkzpRs2UBZDQI77+cT3P6rFCB1A0dTs323s0P8VwKPNxJg7UC76QDbcCRMySUWu6oS1yzTCguRlUYTcidqpeZdtHOL09/z+luPzIHHqB/vQ9rnmKvNPJpGrBJkKfytTOuw9v8frDeZaeH6r4iB1b3IcxXDVBG/cZiVMvhj0/b9SbAbkgN94GUrDjIArHEo49eBMFcYKuLFjOUmbiRuESFn3Rlx1SFNsPk2GEohrRvsb3Fzh9UH6hwKFUEBxwUWIGMtPpf2rIDmUxAEUigjvrWMiGoDk4x5FdM+p5livY9OVeyVGtcfDm8zZJ3psJ6Uz8cqK1ZhYsebZFUup9rZA==.{. "version": 32,. "partner_id": "std-1",. "user_agent": "std-1",. "search_engines": {. "location": {. "ad": {. "other": {. "list": [. "google_com",. "yahoo",. "duckduckgo",. "amazon",. "bing_attributed_ysrcunow",. "wiki".],. "speed_dial_index_list": [0]. }. },. "al": {. "other": {. "list": [. "google_com",. "yahoo",. "duckduckgo",. "amazon",. "bing_attributed_ysrcunow",. "wiki".],. "speed_dial_index_list": [0].

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\T9RRWRNL\features[1].json

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1523
Entropy (8bit):	4.399292637963254
Encrypted:	false
SSDEEP:	24:YPiRyiRAS3R+GRH4rRUtRCRMR6mR9R5DR3RoRY+RWEIiRGiRCR8xRIjRuAcBpDRC:YqRyiRhR/RYRUtRCRMR6mR9R5DR3RoRY
MD5:	B7C15128A1E2AA333069D2797BFEFD6E
SHA1:	5BD78BF3DF58921E80A72895BFDF2DE3F6549A50
SHA-256:	FA5789F32C280FCDEA8E61CA8A322F859390C64CE8776D131CE73421D9882A93
SHA-512:	DCC4EA98D587CDBC7FB21A7EB383938CE70744DF897EC9D8A7BCF1532E1028D0D1395B9732494FC3196AD2D080D33F5F2153A82A3DFC0F2F055D5E31B50DA5F
Malicious:	false

Reputation:	unknown
Preview:	{"features":{"01979299c8cd":{"state":"enabled"},"13e025f64bd6":{"state":"disabled"},"13eeaf851da7":{"state":"enabled"},"15322f489976":{"state":"enabled"},"1ad69 b007ce5":{"state":"enabled"},"1c4dddb65bac":{"state":"enabled"},"1d24dceb937a":{"state":"enabled"},"278deecb29a1":{"state":"enabled"},"2c1429a5a72e":{"state":"e nabled"},"3389f6c15eb9":{"state":"enabled"},"40db6e644d2c":{"state":"disabled"},"50796754ffc7":{"state":"enabled"},"5448a57d6689":{"state":"disabled"},"54726ed4401e": {"state":"enabled"},"56d717ae3ad6":{"state":"enabled"},"5a28d66c82cd":{"state":"enabled"},"603cade21cf7":{"state":"enabled"},"654296fe9d6c":{"state":"enabled"},"818 c3ef12d0b":{"state":"enabled","dna_filter":{"required_dna":["64336fb81a04836eb8108d24fbca3aa3682db0a5"],"forbidden_dna":["5b3eb4a6c335a0659d16d1a189ca 155e4441ea14"]}},"8511df77ed15":{"state":"enabled"},"970fe421a344":{"state":"enabled"},"9ec4e68ae70a":{"state":"disabled"},"b2a2a32b832b":{"state":"enabled"},"b 7751444d14a":{"state":"enabled"},"b9677b

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\data_0

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	1.5782420290561074
Encrypted:	false
SSDEEP:	192:dNYsLXKixA+ibMlwTkPhE2cSsYNEPsqN7l/vw2tvVP94Yo:d+sU+ibXTku2cSvN/qRl/0
MD5:	D23E72F49AC300CB38FE2825115373A6
SHA1:	7903C9A9C53E04F0391B6EA6A4440E237A8E9B92
SHA-256:	BAB3520927A787D7EA3BE12D2918B7F762F5B10E7DC07676CD36DB807AA67190
SHA-512:	6ECAFC811491883D2D72C2E2AA885A0EB69AAD36E813736CDCF70E56EA8D2D49767297D92082E38C196B9C3624EB53C112D5F7881856312996CCA12A54B9A18
Malicious:	false
Reputation:	unknown
Preview:	.....$..... ....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\data_1

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	2.936568291408256
Encrypted:	false
SSDEEP:	1536:nuOeDhYbrHZuiO3qqj/h2am05o22CPa4U:udDhYn5sjq05Z2f
MD5:	E75E88498027D92A327851B2E2C031A6
SHA1:	6D781679929777E5516EA46950EEA90248B32C83
SHA-256:	98AEF573FE0CF675117857492EAF3455955CB5F6ED4F1B21401053964B9F23B8
SHA-512:	C9BBF0902578FACB218FD5A65050000B1F49A62375B7EAF14074DC6158E2AFC1227CFF438637DA3C9EB534469153EB6F968516633EE4C6EC85F54544ED00B950
Malicious:	false
Reputation:	unknown
Preview:	.....L..... ....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\data_2

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	2105344
Entropy (8bit):	4.561363137892783
Encrypted:	false
SSDEEP:	3072:FFRt3PSEq+NnVSx0k7GaXx3GaXx+ddys9Drt5BXuxqYLTa5D6b3lC:FRl+1dMsZt5BhYLTa47
MD5:	673B5E69D1E5190A710CB32A7511AD49
SHA1:	18888ED7FF8A92FE356DFB70AD6EEB857679AC46
SHA-256:	BCB109FC3FAAEE573756EDDC9611802943F652814EB4318E4521C3EC51D62D3D
SHA-512:	B06226D70FF43BF5C09F6536D6F3579C28062FD39E788F1B4D74E8A2FD93D4EED8A22EF2ECA80549C4D5210880EC63BBC3A9176400356270819EC09BA4124F2
Malicious:	false
Reputation:	unknown

Preview:	.....+.....#..... ....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\data_3

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	4202496
Entropy (8bit):	2.251248661269294
Encrypted:	false
SSDEEP:	24576:3Zim3HgR+zL+HSQUNULUFUhURKWLeCn3mXiFcWZ:3Zim3HgUzL+yrLeHyX
MD5:	12B960EC1E9025A1E6406BD7142E204F
SHA1:	AEDE287F0006017D353D5F76087E09123F6217BF
SHA-256:	74E0A626A0CDFD87630A5A59A5BF8F417B65BE41EAF399A2940E383F379E65A2
SHA-512:	AEFD46BE6D9EC3A590789A06DF6185921673C8A9C1B394A8B17BA88433AD9EB918F9A68DF5EA5408AE1AE2309FD79AC16F26977FF4AE6D2EC68998C81ED12E 66
Malicious:	false
Reputation:	unknown
Preview:	.....j..... .....ww...w.w.....w..ws..... ....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000001

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (49525)
Category:	dropped
Size (bytes):	179256
Entropy (8bit):	5.382954896250264
Encrypted:	false
SSDEEP:	3072:lXN5l+PN3NpnQ2oY8IGI3vzL61qsMY2meNkkEDZpu//A/FS5g:l95lgG71qsJIOkEDZY//A/d
MD5:	2AA9094D225A4197394B173E77F8722B
SHA1:	63478FD6245BE38260007E818119EC37A409BBB3
SHA-256:	46C71F4549663C5304CE350447025DB57E8B771D37F2427FE9CABD971F0F24DD
SHA-512:	DF098137B0CD6ACB3D2D2AA6A30A8A3302A74B47E67FADA54E6377F4726790DFE53F6B90BEF7AFEA93DAAD79C54770FBD65929E07BD04A5FEEFA1798763820 F0
Malicious:	false
Reputation:	unknown
Preview:	(function(){try{var e=typeof window<"u"?window:typeof global<"u"?global:typeof self<"u"?self:{},t=new Error().stack;t&&(e._sentryDebugIds=e._sentryDebugIds||{},e._sentryDebugIds[t]="a8225bd0-7159-4e04-9948-78b2d86cb6f8",e._sentryDebugIdIdentifier="sentry-dbid-a8225bd0-7159-4e04-9948-78b2d86cb6f8")}catch{}})();var qo=typeof window<"u"?window:typeof global<"u"?global:typeof self<"u"?self:{};qo.SENTRY_RELEASE={id:"corner-desktop@5.13.0+6626"};function D(){}const Zt=e=>e;function Vo(e,t){for(const n in t)e[n]=t[n];return e}function Wo(e){return!!e&&(typeof e=="object"||typeof e=="function")&&typeof e.then=="function"}function ji(e){return e()}function Br(){return Object.create(null)}function oe(e){e.forEach(ji)}function ye(e){return typeof e=="function"}function Xo(e,t){return e!=e?t==t:e!==t||e&&typeof e=="object"||typeof e=="function"}let xt;function $r(e,t){return e===t?!0:(xt||(xt=document.createElement("a")),xt.href=t,e===xt.href)}function Fr(e){return e.split(",").map(t=>t.trim().spl

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000002

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	183955
Entropy (8bit):	5.132262442335376
Encrypted:	false
SSDEEP:	1536:/ejFU9yb5abYO3/Cg7eEHU+Yz110it7n7MQd2MFN:27b8jGVI
MD5:	CB5DAB4C23CAB678B12A44A03455D6BA
SHA1:	547A8D7056EEAE96D1529F7B2A6EBD64A282888C
SHA-256:	8178D1BCADE69FE8DAF3D49515EDB867E28417C9FCC570920CE814776A98D061
SHA-512:	6015571C82A4DE9EBECF6D8CF84EE7C3F46EBF5328893687E1A9B8D973D90F000A0E0D6C135261E540464165437EEAF8935538801B1D425024A6CB52CF326A8
Malicious:	false
Reputation:	unknown

Preview:	img{max-width:100%}img+h1{margin-top:.46em}.lazy-resolved img{height:auto}html{font-size:62.5%;scroll-behavior:smooth;scroll-padding-top:6.5rem}@media(min-width:1024px){html{scroll-padding-top:7.5rem}}@media(min-width:1824px){html.large-screen-ready{font-size:65%}}@media(min-width:1924px){html.large-screen-ready{font-size:88%}}body,html{height:100%}body{background-color:#fff;color:#000;display:-ms-flexbox;display:-webkit-flex;-webkit-flex-direction:column;-moz-flex-direction:column;-ms-flex-direction:column;flex-direction:column;font-weight:400;height:auto;min-height:100%;overflow-x:hidden}:focus{outline:none}main{-webkit-font-smoothing:antialiased;box-sizing:border-box;flex:1 0 auto;font-family:Be Vietnam Pro,Roboto,sans-serif;letter-spacing:.02em;line-height:1.5;overflow:hidden;width:100%}@media(min-width:1224px)and (hover:hover){main{overflow:unset}}main,main article,main aside,main details,main figcaption,main figure,main footer,main header,main hgroup,main nav,main section{display

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000003

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	PNG image data, 742 x 942, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	110481
Entropy (8bit):	7.948420085309236
Encrypted:	false
SSDEEP:	3072:wN6LzbEzOpFQjuUCKbHig72R4c3C4tshxLvpdl0ifN/:wyEGQjuUCKWw2pTKtdl0iV/
MD5:	CAF9DBA66D56E14DE32D32E040C0D1F6
SHA1:	A69A92EC7719D6992640A8CD26E1501BDF42556F
SHA-256:	CEC63F3EA6863E556F02C79067F2F1E2CF3C18A137126C764C9B7EB0581761F5
SHA-512:	D133E6B4A4FB1632E2F5B4F821E6B1F6435FC5A0EC8716758ECFF245950A6A2A9B7D2CDB52D3DB2F973812EE4BF9B6FA578A2324B54EEDBA840F08ED67A92B09
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.............|;".....PLTE.. !&$'+*-212............:9;..................@=Aqnr....................`^`...NMO......FDG..............ZUZRMXMEK..............B9bqd..{.1*F........!..!..{vz..&Ep.$..'..'..+..+..I..:..x.)..6..G..L..N..A..>-."..4F..1.......>d.%2..6..t.'^.#...1.#.....36.$..7Y.":.%9..\|.)@.&N..@. ...E.*k.&R.%I.%M.-T. @....=p.'U..M+6[.4...idh...b%:\.)e.1...#..g+Cl#;'..*..o,F.....+p.2v0Kj.+2.....u.:...x&B6...0M;...%B@..F..M5Axcj[FQzDW.g\|fOY......_@J..;.8V<$/......D+6L.....fGQ...&FpV^.x...V6By.2....r.Q..u]e....ltgSd.^r=.(V...+Mb...ho...7]\....;i......,P.Ed.Rep.!. ?y.$..*..&.!B.:e.0X..*..-.#G.Es.&L.8e.1[.*R.<kW=Hygz..E.2_.>I.(R.!H.Cu.z..NI.53......gf.-?.PmUf...dw.t..Rh....(.V]....w\|.. .C.GLR.u..n.s`sf\l.(..@..E..3..d*..x..O.W%...1tRNS.....'/;FWf......................................}.......IDATx...[.../4C.RT.f2..t.?r....;C....{....f.m..b...ecK[..<..$...SVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV..h.X.O..

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000004

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	183803
Entropy (8bit):	5.550411005450225
Encrypted:	false
SSDEEP:	3072:vD/LOhR8mEx3cWizJCD6MkEwjsca60yAntQ55:7/LOhR2VJIJVMkqS0a
MD5:	89BB1D0C7C68482CD0C29472820A7EB4
SHA1:	219AE75C8DB6045572D6BB01DFC21A7ACD2B5353
SHA-256:	61E6D1BBC432C3963365A2B7BC166FD83A1B884ED3584EFDAAFF66D24E9A4E9B
SHA-512:	E546660DAE658F3BFBE90B59A7420C09557DA63A3F55848C1905EDC0DE05AFB966F741467F3B625A0D2544458B14A88EA314712960C15DD73B30B89F7FDE0F82
Malicious:	false
Reputation:	unknown
Preview:	!function(){var t={9552:function(t){"use strict";t.exports={aliceblue:[240,248,255],antiquewhite:[250,235,215],aqua:[0,255,255],aquamarine:[127,255,212],azure:[240,255,255],beige:[245,245,220],bisque:[255,228,196],black:[0,0,0],blanchedalmond:[255,235,205],blue:[0,0,255],blueviolet:[138,43,226],brown:[165,42,42],burlywood:[222,184,135],cadetblue:[95,158,160],chartreuse:[127,255,0],chocolate:[210,105,30],coral:[255,127,80],cornflowerblue:[100,149,237],cornsilk:[255,248,220],crimson:[220,20,60],cyan:[0,255,255],darkblue:[0,0,139],darkcyan:[0,139,139],darkgoldenrod:[184,134,11],darkgray:[169,169,169],darkgreen:[0,100,0],darkgrey:[169,169,169],darkkhaki:[189,183,107],darkmagenta:[139,0,139],darkolivegreen:[85,107,47],darkorange:[255,140,0],darkorchid:[153,50,204],darkred:[139,0,0],darksalmon:[233,150,122],darkseagreen:[143,188,143],darkslateblue:[72,61,139],darkslategray:[47,79,79],darkslategrey:[47,79,79],darkturquoise:[0,206,209],darkviolet:[148,0,211],deeppink:[255,20,147],deepskyblue:[

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000005

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	PNG image data, 894 x 512, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	66977
Entropy (8bit):	7.975266461134708
Encrypted:	false
SSDEEP:	1536:/x0sD98c6CqLbdaqk+EzJO3+idGnv8wXYW8reC:p0sD98c6jaTzJO3F+PXcqC
MD5:	D65CF3057A2A83C9084460DF1109F701
SHA1:	C638170E13ED0AD777150E6179A9FB05B0DC4689
SHA-256:	1098BCECE02EFE3B0BC68A26ED1E52E743FB055B4A841850B8868DA2037FF7B5
SHA-512:	8F9EB5F9D363EA6346A9D0E336B3C04AFB46B3E0F378BA5DE0143E19C47B10EE8790D9517AD81A87FBD16AED5A83975B9A1C21DD32BE7BBEF45987C579FAEF59

Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...~.....N#....PLTE.....L..N.....!!!:::..M.....LLL..O..M..M.....L]]]...gggqqq.....us~$-s%/u...>=E!+I&0w/*7=M.#,n#,p)h<K....@P...CS.AR.!*i?O.'1 z..N(2}CT.*5.0<.;J.-8./;.9H..:.4A.*5.)4.DU.6C.,7.1>.8F....+6.7E. (d$&+3@...@)3..'_&(-.....EV....z.-.%[.....##*..!!!'9:B.[+..$.zy)+1.....,3sqoz77?-.5.....44<O]...HJT019..4_[r ..,.....#U@?F)%1=@ILP[DFQ.....mlw@CMLMVEDK...jhq....!O...T."...8A~SQYb`jfdn[Yb....VT_...BK.....^]f..ELU.Zh.....y..;Bs...q}.ou.^e.....-4d1..B.....k.'.....JQx...%..... 9dg.....i$.....W^.....3..KZ...v|.7,*.....E..O.....H^.&*" yx.c;.....Ahp.uG....]f..Y.....w!L/.....TWE43[69.....ur.....P.....jk6.....`a..srsl^XNB?{ke....F.xq=Ch..}_OK.-.... ..rIKy/H..:..E..7....WU....q..<...6Kg.....tRNS.....-=Mat....$k...B.....:...@IDATx..n.@..W..p.....L.m....,.+....JP ..,.....E^ .CAK.EP.....$..v%..o..69N..9s.....{....!.....8.. .0.X\....$.../.H...K...KBX.p.C.rd}

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000006

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (3571)
Category:	dropped
Size (bytes):	260232
Entropy (8bit):	5.548800881054804
Encrypted:	false
SSDEEP:	3072:2AF5QU3Zw2yU/24yI8UNzPQYEFy68aLBO1ggey0enLHW6WEkXqDVRUYodk:2ADw1E4YP9CE1ggey0enLHJWEkXqpR1
MD5:	786FEC25873FD2603E79565E8C650611
SHA1:	EFA5922576665757ED0A5B904BEBF0DE86165ABE
SHA-256:	8D3651B112F945D12CCBCDF9337AB576ACF0E586A3CFDBF3E09B6FFF42328FE5
SHA-512:	D7C41548E3EA8097E5BD6A82680C19ACC9CA0CE8E6D8DD1A270100428C652F648EBDAD8B94CA84F3A940D5F6388676A8B7547B162042E7273F3BC3A9756FDD 6
Malicious:	false
Reputation:	unknown
Preview:	.// Copyright 2012 Google Inc. All rights reserved.. .(function(){..var data = {."resource": {. "version":"49",. . "macros":[{"function":"__u","vtp_component":"PATH"," vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__e"},{"function":"__u","vtp_component":"QUERY","vtp_queryKey":"utm_source ","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__u","vtp_component":"URL","vtp_enableMultiQueryKeys":false,"vtp_enable IgnoreEmptyQueryParam":false},{"function":"__u","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__v","vtp_name":"gtm.elem entClasses","vtp_dataLayerVersion":1},{"function":"__gas","vtp_cookieDomain":"auto","vtp_doubleClick":false,"vtp_setTrackerName":false,"vtp_useDebugVersion":fal se,"vtp_useHashAutoLink":false,"vtp_decorateFormsAutoLink":false,"vtp_enableLinkId":false,"vtp_enableEcommerce":false,"vtp_trackingId":"UA-4118503-39","vtp_enab leRecaptchaOption":false,"vtp_

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000007

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	PNG image data, 683 x 887, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	221871
Entropy (8bit):	7.989927789874321
Encrypted:	false
SSDEEP:	3072:frqmFYD3ZeWfRQna8GwPCWHKftOE0Q7DQyeu4vV08DDLXYSk/VxaSSGkXi7:frjWfG7vvHKh3UzvFDHIXMSSGKi7
MD5:	DA18470476DEB24C61729DE13B781659
SHA1:	594D8E07D1B48914CBB53BB8920B39DF18B7A3AA
SHA-256:	DBE41B786CD6A53BCF72DDB1FAFB4D0A920B8E1F1E7FEF54ACAE1E900D290996
SHA-512:	1D6556E85FA8FF5C772D44C673DABB6BBEE612087A1F6E1D3CF5E2745EBD1278D370614298174A6DFC55EF2A5774535E8C0EE91B71DC6AE78B226D4E3D152E 66
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....w.....bvIDATx...7..!.....J...;x..l.+f..w.....C.....?....m[l....YJ.k.cJ.$..q.....e..`.I.0>.{M..*...IE.^t....l# >.m..].m..'.I..?..._2..._..<;...ell..Z.....9. .cijj...8`.....w#....."...2o.|..B.YH...Ti.\...#..&.\...V.w....5..^.R.....Juu.h..BHV.%.*..D*..U....]...0.....>...}.?.....}..O.....%...9'..B.q.[R R.^YY..z..Lj...."....;.1.....B(VU.Joo.`.aM...ZSS.....>..\...5^X.gL...D...Q.....M.!/...T..A ..B.....h...[:.6,--mG.T3&211. (.FPB..5.+,..r.!.B.....M...g.`.(.....gv...8.X...?...C.....7<.t.. .!...Y..w)//.B3!K4...&Ra.W..Q;[.2..!dA....3.e.W-.2..k..z\E.g}}}..J..+p..S.W__/...fz{{....54....s...?::...:..Y@.{.TBVP...eXq.4....e.h...B.+vhF....];<<.....4.B...`c..UZZ...9.i...S.. .7..R;S...gP...xM.).>)n...fL.....O..._...>("..B...|.r!....._.[WW....=...]...c."p.@....Q..B.-&Va.]M..Kp...0..f.....X..}B..w.'.!.....;.Q3.....".4."....Q...a",..

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000008

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	125667
Entropy (8bit):	5.495889029096188
Encrypted:	false
SSDEEP:	1536:k0ccXHcct/8A4CnW9OqqpLJ31U8i8bqeCuA5qFwENXufuXufu8uY0DguywMWMXZv:vcOcEpN3m8i8OVWXufuXufu87uywtMXl
MD5:	F8990BA62F33CB6E3ADFC6BC34F27089
SHA1:	C5D195A80177649763 94C20CE6F2765CC48E0B14
SHA-256:	5920B740DE64D877C8959FCB54871F598DDCE457E52DCD68309BD21BDE3210D1

SHA-512:	A81184FDEDF0B16E3FB0107DF90F40729B5A6F58A8A3B05C67205B7BBF13721FFA0F8266BC720AFEFB75C8522DF0A604393ADA70003373387BF2BF89FAE327FF
Malicious:	false
Reputation:	unknown
Preview:	.colors.svelte-1kkf556{display:contents}.button.svelte-41rzyv.svelte-41rzyv{align-items:center;align-self:var(--align-self,stretch);background-color:hsl(var(--color-N20));border:1px solid hsl(var(--color-N32));border-radius:var(--border-radius,2px);box-sizing:border-box;color:hsl(var(--color-font));cursor:pointer;display:flex;font-size:var(--font-size,12px);font-weight:700;justify-content:center;padding:var(--padding,8px 16px);text-align:center;transition:opacity .5s ease-out;vertical-align:middle}.button.primary.svelte-41rzyv.svelte-41rzyv{background-color:hsl(var(--color-accent));border:1px solid hsl(var(--color-accent));color:hsl(var(--color-font-accent))}.button.primary:hover.desktop.svelte-41rzyv.svelte-41rzyv{background-color:hsl(var(--color-A120));border:1px solid hsl(var(--color-A120))}.button.primary.disabled.svelte-41rzyv.svelte-41rzyv{background-color:hsl(var(--color-A30));border:1px solid hsl(var(--color-A30));color:hsl(var(--color-N32))}.button.secondary.svelte-41rzyv.svel

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000009

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (46335)
Category:	dropped
Size (bytes):	420014
Entropy (8bit):	5.574785871915572
Encrypted:	false
SSDEEP:	6144:dadWAD/1+bMPeCE1ggey0enLHJOEkXqpVUrp+uPC3:k0WUbMPrEqgey0enLHvUrp9u
MD5:	84D4B8103F7A61D6F7C6E0E363614318
SHA1:	A4F29ABD475FC846284F569AB44F2669D4B29E8B
SHA-256:	E80FBC6FCC47E0A8F31C9390EDBE26C255309473AD22B26BF427E60CDBE71455
SHA-512:	FD438366CEB52CF38D484AE3CBCE157629109ACEB3A37B32876F66C5CB4EE2E34491C5EF0BA81C75F0A2C22890431CD17DE7BA29A0C47B92674F0A4D05C07E25
Malicious:	false
Reputation:	unknown
Preview:	.// Copyright 2012 Google Inc. All rights reserved.. . (function(w,g){w[g]=w[g]||{};. w[g].e=function(s){return eval(s);};})(window,'google_tag_manager');. .(function(){..var data = {."resource": {. "version":"362",. . "macros":[{"function":"__e"},{"function":"__u","vtp_component":"PATH","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__k","convert_null_to":"GA1.2.","vtp_decodeCookie":false,"vtp_name":"_ga"},{"function":"__jsm","vtp_javascript":["template","(function(){var a=\"GA1.1.\";return a=",["escape",["macro",2],8,16],".substr(a.length)})();"]},{"function":"__k","convert_null_to":["macro",3],"vtp_decodeCookie":false,"vtp_name":"gclid"},{"function":"__gas","vtp_cookieDomain":"auto","vtp_doubleClick":false,"vtp_setTrackerName":false,"vtp_useDebugVersion":false,"vtp_useHashAutoLink":false,"vtp_decorateFormsAutoLink":false,"vtp_enableLinkId":false,"vtp_dimension":["list",["map","index","4","dimension",["macro",4]],["map","index","3","dimensio

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00000a

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	Unicode text, UTF-8 text, with very long lines (64032)
Category:	dropped
Size (bytes):	589079
Entropy (8bit):	5.505405618282047
Encrypted:	false
SSDEEP:	12288:NZKiQnsx366wF4TPP1fRW+wgVm/K8lYlE34YunqLfid5dHMi2ZLrv+njVu7NNPXA:Nhkq366wF4TPP15zbVm/K84E34YunqL+
MD5:	E36AB5D5F38B1A9650E8F6979D8A2C26
SHA1:	C15F8BABC6FB4FED0F3E952B37499F88C1640D8A
SHA-256:	91918AE89458C10C420209F1F1A57CB292B5576DDD195473D2538C7EE3819015
SHA-512:	199D0DD038B0C19A4A9405401640C94C4A9FCCC21EA8049872F9EB824C7D71501CDB680613D97A0BA4295BCD0E1C4990355FFFB324F7746C5C7AFF4273E0E18D
Malicious:	false
Reputation:	unknown
Preview:	function __vite__mapDeps(indexes) {. if (!__vite__mapDeps.viteFileDeps) {. __vite__mapDeps.viteFileDeps = ["assets/GamesDeals-Y3izAFyA.js","assets/vendor-riiAV_l.js","assets/Badges-CuIfQk-d.js","assets/Badges-DtURwYrQ.css","assets/index-DtMr64Oc.js","assets/index-BRRDBs1E.css","assets/index-DQE_taSP.js","assets/strings-D9eBrPdG.js","assets/GamesDeals-BUELdmmC.css","assets/Stores-C0USjB1a.js","assets/Stores-f2rU9E8n.css","assets/News-BKO8KtbO.js","assets/news-CDLEvZ7G.js","assets/News-B76hfSrT.css","assets/Trailers-2g7-wYZQ.js","assets/Trailers-D_RtdYi6.css","assets/VideoHero-D4Ko9yo2.js","assets/Hero-KRGNLa6L.js","assets/TempBanner-DUEimgu3.js","assets/TempBanner-AcaA64O8.css","assets/Hero-sTJbxqxT.css","assets/VideoHero-vZN47iXX.css","assets/CollectiblesHero-BLDvEpEr.js","assets/CollectiblesHero-v5epPvz7.css","assets/Stream-CQu19eZp.js","assets/IntersectionObserver-DZG7XBCV.js","assets/campaigns-DNj7talR.js","assets/Toggle-DtOd5MZa.js","assets/Toggle-DVfzmk57.css","assets/Stream-

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00000b

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	101674
Entropy (8bit):	**7.996614094375929**
Encrypted:	**true**
SSDEEP:	3072:En77f4gSxZ6PAGfi9Xhb2Bvnv2Qy/bkcVf:Y77wgByXhKBvn+9wcd
MD5:	0A62F36BB38ED6A98DD74B807EECE6B6

SHA1:	AF24663D2A25C54526A3659337E1A28A729D7C01
SHA-256:	00E676EB239892B91B389AE4EE0FC68A9451661E28F47799FBD89FBB87357E68
SHA-512:	111057C82D6B1C89EB070C0101853FC4C15398A4AB177CF692B6AA7BE6C9B1138D22ACA06CE99CE1B25F5FC55F3AEAC7D9FB3724FEB8850BF020E5B323983BBF
Malicious:	false
Reputation:	unknown
Preview:	[..4.i[Ls...l..C.(l...*...:.c.....1...e;.....f.??_.;mgS2^...G..N.$.L.bT.....$....O.....|5ur8U.e.....c..8d"l_..6C..6u....oC....k..Q...mj0"B.r<[.|.s.....Y...|..^M.p-.....Lr.....TR.$@.Yz..2.dk{.W.)0.g..:.h..M...M..^.u.6(...q...\|.}.J.....6f...R.& .....B.....U..%.....s*s.e.lJ...9.nu...{.3._.....2>@. .....@Q. ....CJQ=$..#).WP.AE...(#....}.Z)EvwDT.3..=..x5c..g.k.s.1g.....t.@.@.....G.5F.....1...../.Ywo2.B.....Y...j*!0@../...,...a...o..Y.MK...-...<...n)Z...7....._B.!.....K..|...3.4...#.....r8Wj.}..k>.....e.....nX.....7.U....`8....ya.i.d0...Chw....7.....C8..g..@.,....80.r.._..X..\.,%....>....J...C.\.....n....".....Uj.....`.....y8...+..|..*|B.U.Y..@RJ.:.....<.,.....L.0.....\.g.M..6.v.b..;..h....5...e.F{.....@..no6.....7.Kgb.q..\....+....7J%=..P,..'O.....<p.eZ...c0Ke.Z.....RZ..x..q.....,w...J....\+..uo.f.X..j..r.~x....:r.l.T.....[.|..-R.m...d.-.|.u.KU.m.PH.....D.C.....F.3...^Q..-!.....|p...k}

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00000c

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	Web Open Font Format, CFF, length 61432, version 0.0
Category:	dropped
Size (bytes):	61432
Entropy (8bit):	**7.993923310479825**
Encrypted:	**true**
SSDEEP:	768:+3lo4MuQ2Vyq1qjPpFVHTYacNa9qH2Pm4F82dUK9wlPt1jqhj9dzF2L0qxo1Ji+b:Wlo/uQ81WPASqWPdJUZjojTKQGtojeaX
MD5:	4F566BFD43217D65E8F9D0BC48210E58
SHA1:	F7FCCFEAA774D87B004672030CB9265F2CF991A2
SHA-256:	725F78069005B7469C0A72C4BDAABDE9E930BAE2486E99FE4CB3BCB32D243A49
SHA-512:	E6E9F8EC993FF4CFE328C569F4FEF40438CF0957057B07ABFB0B7A9626FAA347991DCDF3324999526D457602D641583332A5E69D81A512ECF936E31BA017875B
Malicious:	false
Reputation:	unknown
Preview:	wOFFOTTO.....CFF .....'....*T.5GDEF.....*.*.GPOS...4..A}.....d.GSUB.....9|..OS/2...|...V...`].l.cmap.....RT.cvhead.....6...6*..Bhhea...T... ...$...thmtx...X.....V.maxp...t.....P.name.....;....post...t..... ...2.....L.ZX.2_.<.....B.....4.....x.c`d``.....&.%.O.EP..^.....P.....x.c`f.....).....B3.1.1*100q3.031.1.....o&f..z.'..0.(00L..1y..d..r..#i....x...r.F.E....L...qO...a..O.....C.....NB...?...A...J.....7..|.....=\..^._*...~P>...|.....O.....~R...^.....+.w..pg....+..pEy.....~.._)..r.P>.-.'...7*....U+.....7....p...'.C..+..|..nO.(.....Ar:...d....]W.5..iT...en.I..^&%..1.`.Y.{*...RP....~.....\i....W.<..M..J.....~<+;..k..L.n.....Q.d.-..iV.\S...z.#.f[..o.ExH..|.!&.!&'..%=...^..Qq.S...t!..Oy..Q..p...LXa..y.....S..^.!...Z.f..I.(=..!.T.....,..{..x...r..<?'.....I.s-.<2.....UoGUO....`e..,..d.Ho.....Op..Y'.cK...Mx.G.xX....`.....w.

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00000d

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	Web Open Font Format, CFF, length 55672, version 0.0
Category:	dropped
Size (bytes):	55672
Entropy (8bit):	**7.99177392657553**
Encrypted:	**true**
SSDEEP:	1536:hynrwsvx0C2DJkoGtnVF/gBikYVQGtZE9bw6g:gvx0C2DKooV9FTZE9b0
MD5:	04F8526527253346D793008EA8590C5C
SHA1:	CA301ED4559FEC081BA2CE4014734F5EADAA7361
SHA-256:	3EBBCD0A4043F8D291103EBF9B526EF8311A8F5C3525AF83DF586F30F9B32F4C
SHA-512:	F1FA31CA09BC649AC81ACE4C7E5094D09C79D6AA382826FAB7DF3B455E113108180A1DA84E5DE05023970F4FF606EE6C74812AB9C068B037511FC9235D04AF03
Malicious:	false
Reputation:	unknown
Preview:	wOFFOTTO...x.....CFF .....{.....cGDEF.....*.*.GPOS.....9....<S<..GSUB...4.....9|..OS/2...|...V...`[.k.cmap.....RT.cvhead.....6...6)..>hhea...T.....$....hmtx.....maxp...t.....P.name.....MD.}.post..... ...2.....L...=_.<.....B.....U.....x.c`d``.....]8..EP..^.....P.....x.c`fjf.....e.....X....X.r..H.....7....=....U...&.....)..n....x..x.....F.E..03..W.ff,.....K.8...N..HQ..l!.nuI...V.....D5.....q..m\|.....#..p...._...l\|..q..%...3.....3.x2..8..F.....<.}b\|./.O.....qQ.....r...E,.../.?.}m\|..>.M.\|....\`...8.\|..,.-.g.....a.3..8....4l.~..b..I..~H....iS..9..S^.3....T...P.#...=.q..y..M.V.....H..3.~[.r.^...$..W.~.EQ....}.{...^*.y.i.)X....o.....;..K8s.Y.M..GJAKJI..5.....Z..}l.....Z\AC.c.=...1>... %..Y..i).c..y.R2.....Xe!.:pK...z..,..xI.{..o.+T:c}..I..S{.ve.....J.:.^.....V{jX.i.!Z.z.....A.z.h....y...

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00000e

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	134597
Entropy (8bit):	5.836641103005388
Encrypted:	false
SSDEEP:	1536:A6ZPsROeREN3pnqPjuZUPAjfkK5wTYlJkFuW6AUyh1E7slw90dI0DZ2W9u3frAod:JPsQeRE5pqbZFuW63EGj0XQ3TAhmB
MD5:	263D6854FEDAD9A8786A6EF0B4E4A17E
SHA1:	C785370539F04E145B2654012FB239BB13B876C1

SHA-256:	C9C97A443E09F3EB398FC6E958D8F24C88D85FCC68017B1FB8D40C766EA425FD
SHA-512:	03850F93F9AB207D7A417948EB40C1402E3AAAD4B58E923C5332E7DD7D1F57CC8B52E07694D87C853C0AD5FAC9A1697461F22E210503DF9607FF836DD7B844E
Malicious:	false
Reputation:	unknown
Preview:	<svg width="54" height="13" viewBox="0 0 54 13" fill="none" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">.<rect width="54" heig ht="13" fill="url(#pattern0)"/>.<defs>.<pattern id="pattern0" patternContentUnits="objectBoundingBox" width="1" height="1">.<use xlink:href="#image0_501_2684" t ransform="matrix(0.00067089 0 0 0.00281635 -0.178405 -1.97834)"/>.</pattern>.<image id="image0_501_2684" width="2012" height="1508" xlink:href="data:i mage/pngbase64,iVBORw0KGgoAAAANSUhEUgAAB9wAAAXkCAYAAACIcHBlAAAACXBIWXMAABYlAAAWJQFJUiTwAAAAAXNSR0IArs4c6QAAAARnQU1BAACx jwv8YQUAAYhuSURBVHgB7N0JvGVVfSf6/9rn3KnmuQoKKJAZZBBRQIlWHFAalclb0RANKhSKkoS0nU53v/7k+nl5n3TnvZekY3cSSWJ8sdPpR3WGT+zEtk2U7pjBJCqiiI hgMVRRVEGNd75n79XrVGFiGweGurfu8P3Cueecfe49Zw9rr31q//ZaKwIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00000f

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 3840x2160, components 3
Category:	dropped
Size (bytes):	283555
Entropy (8bit):	7.7925810252662115
Encrypted:	false
SSDEEP:	6144:/LchEVc7hRYnBKJUp4L8bKd7bij1/Ghf79WY9:6EV9BUU/2d/ijJGhf7N
MD5:	1E8577FAF290C64DBBA7D4A9C43F34CE
SHA1:	1D09B842B15E59908E810CF361E82749AA20B8D6
SHA-256:	7F147B5C47A4CE283D8AE5D0675E2D02A5EE1541083706BE611BFFC58E27DEBC
SHA-512:	2598D9E7CC5061396EA01B88C7C00AB53F39B7A7DAB68AAAFABA6B538DE56BA981FEACDA0319497833244AE98F4C83801DF3E997317125D137ABC094A669AC 7B
Malicious:	false
Reputation:	unknown
Preview:	......JFIF...p..T."...`.....X..Ye.*.J%...@..T.( .....,.J..(.*P........X.,......@....T(S......@.RY@...%....K8.....J.D..XY`....%%...K..%..J.(J..b."......*P....X,....&9.XP...f@...AB../......%K,.........V.%.@......JB...*X.....),(.P..e...@.... IR..e..,P..@...D....&Qe.......T.(..Tuwd...P......J....[K..8@...@..E.....X...,,.*(K..K.K.,Y@J..PJ%..(........(.P........J.d.P--U........(P.,.QQ@.....KV.!8@....e.X..H...%....YBP.,..% J..%J.A)*(.........K.......@.....(.YeR..P.e.n~.N..... .,.IK,...P.UZ!.......T..H..R.........JJ.,...RRPJ....J....@.,."...P..VY@.YR...,,(...V...:{,.`(*Y`.T.eX.,...Aq.h.#.....H.......X......J%.E ...Q(......P..J...l),....b...@,..RY@*P.J.U...m(,.(......P...X..(..$@.-T".x..".%..T..JK.....(...E.P..)*Q(....P.......(A*...Qe.P..Qa@X..U.*.2.h..Jz........X....I....a......B,....@.)...

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000010

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (65450)
Category:	dropped
Size (bytes):	225445
Entropy (8bit):	5.378711341053158
Encrypted:	false
SSDEEP:	3072:yhwvwV82wOdix0bgz6Fk7YLUaLdmBRDYH:yhwvwUOExEQokbasbDYH
MD5:	645FC548E91F44AA4E1226EE86502370
SHA1:	E4075A2E73B3AB050D85F985847E5DB554B3B2C2
SHA-256:	6265CA724F73E24568A94C7EA752B44E491C10231BFC8E80E86CD3F02EAB2E71
SHA-512:	F6E58EFE8E5B084703B995C644C4D530F4955909DDBBB23E21F8939DD6C8D57C82A62E249561D4B1CDCDEFDCB42C1747CC166145A936A928C59CC53B51E23 DE
Malicious:	false
Reputation:	unknown
Preview:	/*! For license information please see modules.ad6500eebe72fe1c39dd.js.LICENSE.txt */.!function(){var e={4788:function(e,t,n){"use strict";n.d(t,{s:function(){return r}}) ;const r=Object.freeze({IDENTIFY_USER:"identify_user",AUTOTAG_RECORDING:"autotag_recording",TAG_RECORDING:"tag_recording",HEATMAP_HELO:"heat map_helo",RECORDING_HELO:"recording_helo",REPORT_USER_ID:"report_user_id",MUTATION:"mutation",MOUSE_CLICK:"mouse_click",INPUT_CHOI CE_CHANGE:"input_choice_change",KEY_PRESS:"key_press",MOUSE_MOVE:"mouse_move",RELATIVE_MOUSE_MOVE:"relative_mouse_move",CLIPBOARD: "clipboard",PAGE_VISIBILITY:"page_visibility",SCROLL_REACH:"scroll_reach",SCROLL:"scroll",SELECT_CHANGE:"select_change",VIEWPORT_RESIZE:"vie wport_resize",SCRIPT_PERFORMANCE:"script_performance",REPORT_CONTENT:"report_content",INSERTED_RULE:"inserted_rule",DELETED_RULE:"deleted_ru le"})},6939:function(e,t,n){"use strict";n.d(t,{f:function(){return f},W:function(){return g}});const r=Object.freeze({LIVE:"LIVE",REVIEW_WEBAPP:"REVI

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000011

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	27345
Entropy (8bit):	5.24905475138269
Encrypted:	false
SSDEEP:	768:dN+U897o0wh+E425S5zMrPbIFQvtGava1rx4hCbeKkevF3:dN+U897o0wh+E425S5zMrPbIFQv4Sqr5

MD5:	183ADEF418CFCAC3919538D9ABC9AA91
SHA1:	278FC89727946E6B860B253A6CFB28CC2E07CFFD
SHA-256:	0504371CDF41E78C944F76FA3E7D145913D00157C9CA2DD5DAC12EFCEF78331C
SHA-512:	A9B42B8A9BF484845178174904A4AFB092F4FA6540C8EAF693E0ACF5C974872EE19BEC91D6127DC4AC3F07515C34C02752FEDA83B96565E203DCB3AA566E3F6D
Malicious:	false
Reputation:	unknown
Preview:	{"data":{"id":5,"order":24,"key":"gx-corner-videos","publishOn":"both","shuffle":false,"countries":[],"excludeCountries":[],"createdAt":"2023-08-25T13:24:41.885Z","updatedAt":"2024-03-29T11:14:09.915Z","publishedAt":"2023-08-25T13:25:04.846Z","notifyDate":null,"hideTitle":null,"debug":null,"design":"both","sectionType":[{"__component":"sections.trailer-section","id":1,"trailers":[{"id":1762,"trailer":"{\"url\":\"https://youtu.be/FgDYQ3MVsLE\",\"title\":\"The Mind-Blowing Creations of Hideo Kojima\",\"thumbnail\":\"https://i.ytimg.com/vi/FgDYQ3MVsLE/hqdefault.jpg\",\"mime\":\"video/youtube\",\"rawData\":{\"title\":\"The Mind-Blowing Creations of Hideo Kojima\",\"author_name\":\"Opera GX\",\"author_url\":\"https://www.youtube.com/@OperaGXOfficial\",\"type\":\"video\",\"height\":113,\"width\":200,\"version\":\"1.0\",\"provider_name\":\"YouTube\",\"provider_url\":\"https://www.youtube.com/\",\"thumbnail_height\":360,\"thumbnail_width\":480,\"thumbnail_url\":\"https://i.ytimg.com/vi/FgDYQ3M

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000012

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	66786
Entropy (8bit):	5.256787707031287
Encrypted:	false
SSDEEP:	1536:c5+cGw/5f5vfaH8x77vtGg7iCMmKSzBjYhj+9r1IgtDxeyPb5aTS+7GYGALBJ5cE:gfRfJMWtDx4
MD5:	067383EDDB64CDA7E25E5FCD91D96C6E
SHA1:	756A5CC020D3E0295C3E5203AC1092247FF1466B
SHA-256:	3A77E980102F32CB0ABB77036078684BFCDCCE9BA01EE343A4A1B245E4D7E556
SHA-512:	56E57CF4CE94F78798420A2F6BCAA4494A0329A5033510939326CA2C76ADC001F5192931F2619A4C3CAB8386341927EF600CEE4C8325F433BA32F283D1AD838D
Malicious:	false
Reputation:	unknown
Preview:	{"data":{"id":3,"order":27,"key":"gx-corner-trailers","publishOn":"both","shuffle":false,"countries":[],"excludeCountries":[],"createdAt":"2023-08-25T12:02:56.236Z","updatedAt":"2024-03-29T15:45:12.075Z","publishedAt":"2023-08-25T12:02:58.508Z","notifyDate":"2023-11-09T15:00:00.000Z","hideTitle":null,"debug":null,"design":"both","sectionType":[{"__component":"sections.trailer-section","id":2,"trailers":[{"id":1792,"trailer":"{\"url\":\"https://www.youtube.com/watch?v=Pzgopn35Gdk&t=35s\",\"title\":\"Maniac - Launch Trailer\",\"thumbnail\":\"https://i.ytimg.com/vi/Pzgopn35Gdk/hqdefault.jpg\",\"mime\":\"video/youtube\",\"rawData\":{\"title\":\"Maniac - Launch Trailer\",\"author_name\":\"Transhuman Design\",\"author_url\":\"https://www.youtube.com/@TranshumanDesign\",\"type\":\"video\",\"height\":113,\"width\":200,\"version\":\"1.0\",\"provider_name\":\"YouTube\",\"provider_url\":\"https://www.youtube.com/\",\"thumbnail_height\":360,\"thumbnail_width\":480,\"thumbnail_url\":\"https://i.yti

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000013

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	34076
Entropy (8bit):	5.288711600282534
Encrypted:	false
SSDEEP:	768:9IC0lzJ8n2ED9Mf1gjtCeijvcb3095vO0JTzQUVA9+GGff:9IXzJ8nH+fNeacbEvzTzQU+9+Gif
MD5:	01BC5D63FB3DECE27116BB520C2F6DEA
SHA1:	A699E6EC5AE2782C99CE45924C0CF47F5ACEC777
SHA-256:	CB693F0A8F5A3907175AB18582220296B0DA568BAB242BE9B37A5F8F2474BDA0
SHA-512:	1689106225AB144D6469461310B72E3B079CE6ABDBB59878F117E4108C27AAA13AF24D511B3DFBD1BF77BCAB6D2AD7B9EE490BFAFDEBDA5F7ECC475AF2A193A8
Malicious:	false
Reputation:	unknown
Preview:	{"data":{"id":8,"key":"gx-corner-upcoming","shuffle":true,"sectionType":[{"__component":"sections.deals","id":2,"filterBy":"platforms","badge":"genre","popUp":true,"tile":"regular","tagType":null,"globalTag":null,"games":[{"order":31,"id":446,"url":null,"game":{"id":1327,"title":"Terminator: Survivors","website":"https://store.steampowered.com/app/2617340/Terminator_Survivors/","imageOrigin":"https://www.igdb.com/games/terminator-survivors","releaseDate":"2024-10-24T00:00:00.000Z","rating":null,"genres":[{"id":1,"name":"Action","localizations":[]},{"id":2,"name":"Adventure","localizations":[]},{"id":26,"name":"Survival","localizations":[]},{"id":28,"name":"Open world","localizations":[]}],"platforms":[{"id":9,"name":"Windows","icon":{"id":123,"url":"https://proxy.gxcorner.games/resizer/assets/obraz_2023_08_21_154708998_8ba128313e.png"}},{"id":6,"name":"Playstation","icon":{"id":120,"url":"https://proxy.gxcorner.games/resizer/assets/obraz_2023_08_21_154553319_59d8559097.png"}},{"id":10,

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000014

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	Unicode text, UTF-8 text, with very long lines (46429), with no line terminators
Category:	dropped
Size (bytes):	46430
Entropy (8bit):	5.303853365298302
Encrypted:	false

SSDEEP:	768:OaOFhhR5OlahpjfRys3LzQR04TYYyDMOWPKQ:OaOFnRqDRtzQ64IfWiQ
MD5:	72BCA04FD669EB89FC65D59052D0FC00
SHA1:	27E60AEF86F0CB1B2F6B6ED9DF9A4E3BA88EFD21
SHA-256:	823804A7807864B44093A3843788F4CD076E89CF4A6FDEB8D153AE5C2C2DF721
SHA-512:	56058E4C927563CA37DEC4979AF28A415EA3042A389C0BA22738C76D39131317A703A38A95EAB9D913F116F7C2D1DA62A0A87750F47DECA2DDB3447D64303B1
Malicious:	false
Reputation:	unknown
Preview:	function UET(o){this.stringExists=function(n){return n&&n.length>0};this.domain="bat.bing.com";this.domainCl="bat.bing.net";this.URLLENGTHLIMIT=4096;this.pageLoadEvt="pageLoad";this.customEvt="custom";this.pageViewEvt="page_view";o.Ver=o.Ver!==undefined&&(o.Ver==="1"||o.Ver===1)?1:2;this.uetConfig={};this.uetConfig.consent={enabled:!1,adStorageAllowed:!0,adStorageUpdated:!1,hasWaited:!1,waitForUpdate:0};this.uetConfig.tcf={enabled:!1,vendorId:1126,hasLoaded:!1,timeoutId:null,gdprApplies:undefined,adStorageAllowed:undefined,measurementAllowed:undefined,personalizationAllowed:undefined};this.beaconParams={};this.supportsCORS=this.supportsXDR=!1;this.paramValidations={string_currency:{type:"regex",regex:/^[a-zA-Z]{3}$/,error:"{p} value must be ISO standard currency code"},number:{type:"num",digits:3,max:999999999999},integer:{type:"num",digits:0,max:999999999999},hct_los:{type:"num",digits:0,max:30},date:{type:"regex",regex:/^\d{4}-\d{2}-\d{2}$/,error:"{p} value must be in YYYY-MM-DD date

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000015

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	Unicode text, UTF-8 text, with very long lines (22644)
Category:	dropped
Size (bytes):	126185
Entropy (8bit):	5.2840701881480125
Encrypted:	false
SSDEEP:	3072:DBKvA9/BxPCqH+/UQzVqSpXUK0EbuY7f2/X/eY:D7QESpXUK0EbuY7sXT
MD5:	FE9F1F0FF513C519198BAC39FAF30BC9
SHA1:	69B52E582BA19093697935301FE5A6EC96092307
SHA-256:	0A95F5AC572DE9D9DFD32FBFAA58C872067E3BE9FAA594BD85462028C3156470
SHA-512:	D3F4A032F3B29E85D4C704183A3377C48E0A60F386D5AB78182056749EB7F30408C9B220A183652525ECBD220927EB3797FC134C958AF3FCA753BBDC11C5F68(
Malicious:	false
Reputation:	unknown
Preview:	(function(){"use strict";try{self["workbox:core:7.0.0"]&&_()}catch{}const Xa=null,vs=(t,...e)=>{let n=t;return e.length>0&&(n+=` :: ${JSON.stringify(e)}`),n};class M extends Error{constructor(e,n){const r=vs(e,n);super(r),this.name=e,this.details=n}}const er=new Set;function Es(t){er.add(t)}const re={googleAnalytics:"googleAnalytics",precache:"precache-v2",prefix:"workbox",runtime:"runtime",suffix:typeof registration<"u"?registration.scope:""},Yt=t=>[re.prefix,t,re.suffix].filter(e=>e&&e.length>0).join("-"),xs=t=>{for(const e of Object.keys(re))t(e)},We={updateDetails:t=>{xs(e=>{typeof t[e]=="string"&&(re[e]=t[e])})},getGoogleAnalyticsName:t=>t||Yt(re.googleAnalytics),getPrecacheName:t=>t||Yt(re.precache),getPrefix:()=>re.prefix,getRuntimeName:t=>t||Yt(re.runtime),getSuffix:()=>re.suffix};function tr(t,e){const n=new URL(t);for(const r of e)n.searchParams.delete(r);return n.href}async function Ss(t,e,n,r){const s=tr(e.url,n);if(e.url===s)return t.match(e,r);const i=Object.assign(Object

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000016

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	PNG image data, 192 x 192, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	19701
Entropy (8bit):	7.973255823764334
Encrypted:	false
SSDEEP:	384:biAWCmZQe2V/ILPGDH13ufLUFRACRMU6LYRJHXK96dw:FaL2VADGx3uzAAuF6Lj6dw
MD5:	D72CDA1BCB01856F53AB901B70917BA6
SHA1:	C0A9FFA00433A04FCEA1D655AE02B25F5039FE56
SHA-256:	9FACE54CA63E996D2169BDA0C4B9A90353B140FC800AEEDE8B48696C4F64F471
SHA-512:	13743EB949B90BDA73B6271B93D2417982632442DE132ECDE5D6124F4BB9916576E0F49163B6846BBDED2420689528849B46B6678CD941BC9AEBAF9E0570F93D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....R.I...L.IDATx.....1.D..Ys.....J.S..{..nX..h.{...@.H.*..Y.S.k~..y{'.YU.>..g.zvW.....0..V.i.g]...w-.]1.2P...?t.....W....g...%Y.peU....c[k..5...m[...vW.3s#.....;.]g...A..."G$.HNU.941^B>..jX.h'CC]2.....Q...6.1V.../9.1Ke...=d..H..B.0.KT.M.j....0...-S..s...Y<w.l6.....i.BB<.....X..^Nv.M..d77..U.x...t....a..*..1.1.D7(..+.... ..qT#.Mu.z.e..g]\|.dQ.p.b.:...Hz"H.P..z .....Cz\|....[....~.G.eC.."l.&IDc....-....".K44.c...b....../..[..F=A. T..]....0...Di..H..v...S..5.hg.K...t.N....w... ...&=].._..{.....\|..c. ..YU`...y.WSQ$<.^....*...-..N.6i.....]p....h.....,u.@...C,.#..r!..p._not.L....`l.t.P...w#.S.lx.,.i..Y.....k.....x=.....DoG!.. ..".q..@.IM.g.M....y.A.r.@...bH.B...[..#e.W._....^J.R.t{.....+ ..08V6....x...lhn..)+..l.R.A.....U.y.....p.9...}..tz4... ...E.C./?.....nLw.Lqn$....DU.PC~.U.b.c..1.C..."...(o..kT...+...0.N.c.f...-L....7..!..{..._.t.t.h...P.B.o.:....%....o..G.....>.HE.g..6..6_

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000017

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	51779
Entropy (8bit):	5.337745061554449
Encrypted:	false

SSDEEP:	1536:W1aGo6wCE3mFl4WMmcwqW/d5OUo00pDSsRtzxSunThVK:Dtd9hQ
MD5:	67CFF6DB3C62C9A78691EAA28D7C9E37
SHA1:	9702228C44E5FEFB0AD99235E1F72A9553506A2A
SHA-256:	B70E17C4E92A0C04DB6BC92FE82C1CECFA3D7742CDFC89ECA498E328AC7CD1D0
SHA-512:	3C1D1BA5F3350D535C36012A5566C0EB95767F241A5B6248C524F4CAED92A58C34C0DFF65ED26F23653B330388A5421CEEDF1C6BCEA6A1C8F647C7ADE169A8A7
Malicious:	false
Reputation:	unknown
Preview:	{"data":{"id":14,"key":"gx-corner-free","shuffle":false,"sectionType":[{"__component":"sections.free-games","filterBy":"platforms","tag":"horizontalAndSub","tile":"regular","globalTag":{"id":6,"name":"FREE","color":"#b81124"},"globalSubTag":null,"popUp":true,"badge":"store","games":[{"id":216,"order":1,"publishedAt":"2024-03-28T15:50:00.012Z","game":{"id":1429,"title":"Islets","website":"https://store.steampowered.com/app/1669420/Islets/","imageOrigin":"https://www.igdb.com/games/islets","releaseDate":null,"rating":81,"genres":[{"id":2,"name":"Adventure","localizations":[]},{"id":57,"name":"Metroidvania","localizations":[]},{"id":16,"name":"Platformer","localizations":[]}],"platforms":[{"id":9,"name":"Windows","icon":{"id":123,"url":"https://proxy.gxcorner.games/resizer/assets/obraz_2023_08_21_154708998_8ba128313e.png"}},{"id":10,"name":"Xbox","icon":{"id":124,"url":"https://proxy.gxcorner.games/resizer/assets/obraz_2023_08_21_154736126_5b54cab834.png"}},{"id":7,"name":"Switch","icon":

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000018

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (16407)
Category:	dropped
Size (bytes):	16408
Entropy (8bit):	5.909998053301081
Encrypted:	false
SSDEEP:	192:Aq3g0E5Tz5TUPbaEMpPbaEMYmbEXnMxxakyFNtKLuqVJttxDx0hbA:L3gR5f5AmhmF4K4kyFnuX/
MD5:	8F088FF9EE5D46C1FCD3BA3DD2C7DB02
SHA1:	E5E544458BF173FF85B92A06BDCCEEA4A95B0D71
SHA-256:	75778581A1075C0E377F170167C582094C9D99CC8C013AA2007CEAC957A00399
SHA-512:	B5793DD6ED3C22AD53E6AC47808E0B019B8E033B0DB3EBEDA493DB45FC1230360BACA395133E2718115166779901944AFA76C7580AA45EFF285F1A981593A0B5
Malicious:	false
Reputation:	unknown
Preview:	.link.svelte-13hojts{background-image:url(

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000019

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	47661
Entropy (8bit):	5.327718495226229
Encrypted:	false
SSDEEP:	768:OSb3095ftBjtCw0yQUUeYvsk0ucNUk6/g0rgAv2bbm90jcqi9ysw7ae3YG0ZQ9Et:OSbEft3mUUeYvsk0XNUk63gAv4zc7w7W
MD5:	2188A58A16B2F6DF124BAD4233CB6256
SHA1:	6B0D2BC4EDFA662067E8C8928A33176B361C9B71
SHA-256:	3134131897B5ED9B45D64F9E1CADF57DB88CEA8125BEFF9B03FFBD4C402486A7
SHA-512:	84B022039248C7E611E0CE4A8B095B3F80CAFC0BB86F743CAA68DBCC861AF7978E0788DA78F99F15863EECA319C6A797803B786E7424DE90BD0C85B26D03570C
Malicious:	false
Reputation:	unknown
Preview:	{"data":{"id":10,"key":"gx-corner-top-april","shuffle":true,"sectionType":[{"__component":"sections.deals","id":4,"filterBy":"platforms","badge":"genre","popUp":true,"tile":"regular","tagType":null,"globalTag":null,"games":[{"order":1,"id":479,"url":"https://store.steampowered.com/app/1733240/Phantom_Fury/","game":{"id":1373,"title":"Phantom Fury","website":"https://store.steampowered.com/app/1733240/Phantom_Fury/","imageOrigin":"https://www.igdb.com/games/phantom-fury","releaseDate":"2024-04-23T00:00:00.000Z","rating":null,"genres":[{"id":1,"name":"Action","localizations":[]},{"id":2,"name":"Adventure","localizations":[]},{"id":22,"name":"Shooter","localizations":[]}],"platforms":[{"id":9,"name":"Windows","icon":{"id":123,"url":"https://proxy.gxcorner.games/resizer/assets/obraz_2023_08_21_154708998_8ba128313e.png"}},{"id":6,"name":"Playstation","icon":{"id":120,"url":"https://proxy.gxcorner.games/resizer/assets/obraz_2023_08_21_154553319_59d8559097.png"}},{"id":10,"name":"Xbox","icon"

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00001a

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data

Category:	dropped
Size (bytes):	116276
Entropy (8bit):	5.353899176843121
Encrypted:	false
SSDEEP:	1536:CYHgLADrKm6KluRvspTTumz1dv9R7v7FEpMSi4eortzKtwy6pt8S7a/dSjKke8G8:8EpFMD3gyP1
MD5:	7A5C316861A951EFEBA06DECFF20C59C
SHA1:	1A76A07EEFBCE8A0E4BD092CF9B1696EAC8C7F21
SHA-256:	641B3D4BF69D298E85E50637672EB58AE90FB50EC06459194EEE9887A1774EB5
SHA-512:	3638DF6A72526565716EFABF24B3D2AA1919058A0D2E6A6FBDDDC7B71A0B7A52D1A6F54A5CDA7B237709B409D716DFBC2F3E17F86BA26251305009B292EA1B5 7
Malicious:	false
Reputation:	unknown
Preview:	{"data":{"id":88,"key":"gx-corner-daily","sectionType":[{"__component":"sections.daily-section","id":1,"topCommunity":[],"items":[{"id":214,"key":"daily-meme-graphics-upg rade","visible":true,"publishedAt":"2024-03-09T06:00:00.000Z","dailyType":"daily.daily-meme","title":"Graphics upgrade [meme]","category":null,"description":null,"locale" :null,"label":null,"reactions":[{"id":46,"name":"Rambit 4K","emoticon":"https://proxy.gxcorner.games/resizer/assets/operagx_4k_b99dd2a3f0.png","count":462},{"id ":25,"name":"Aura LOL","emoticon":"https://proxy.gxcorner.games/resizer/assets/gx_Aura_Kek_825b2826b1.png","count":3433},{"id":62,"name":"Rambit Monka","emotico n":"https://proxy.gxcorner.games/resizer/assets/operagx_monka_4cb62c8907.png","count":508}],"backgroundImage":null,"image":"https://proxy.gxcorner.games/resizer /assets/download_194af154d0.png","video":null},{"id":221,"key":"daily-cowboy-bebob-overwatch","visible":true,"publishedAt":"2024-03-09T14:00:00.000Z","dailyType ":"daily.daily-regul

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00001b

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	69385
Entropy (8bit):	5.276789500895045
Encrypted:	false
SSDEEP:	384:PAgIUnYBklCvKr1XicZuyS3IUM1tZfLdt1/obYz+DZL6FtEoHBKwBbHjOsTPOTOb:3Kr1X9S3TMbDobL6FTXxW+ozLEsbhG
MD5:	AB8EBF636E729F8FCE0A9DC9D0C66953
SHA1:	728BF004E25D1A22DA9647B441829B5A01835AFE
SHA-256:	EDB16AC11F09CAB4FC7A5383B9FAF0A09256D3886AD6A9E5B92931A6005C9896
SHA-512:	21C1F218A3B06541B1930B40D5E29F790F74D0DD3B60A3FCCCD38EE86732C40B16D5F59F4B4DBE228D9435D3BC81E0D3959BDA9BE87BC0C21F01578B05BA06 E3
Malicious:	false
Reputation:	unknown
Preview:	{"layout":"category_grid","news":[{"article_id":"9aa4b37391115a32d74c16db33982592822a9b30","display_url":"https://www.esquire.com/entertainment/movies/a60341611 /jordan-peele-us-anniversary-restrospective/","image":"https://discover.operacdn.com/assets/tn/l/mq/9aa4b37391115a32d74c16db33982592822a9b30","publish er_domain":"www.esquire.com","publisher_favicon":"https://sd-images.operacdn.com/api/v1/images/aacb366c74913d44dc504e9eee1232dc62f9ff1b.png","publishe r_name":"Esquire: Entertainment","real_url":"https://www.esquire.com/entertainment/movies/a60341611/jordan-peele-us-anniversary-restrospective/","size":[1,1],"t emplate":"default","title":"Jordan Peele's Us Is Still Scary\u2014and Relevant\u2014as Heck"},{"article_id":"3cd91f5d8f6cbd11bbe0d591c4d4545ab208be56","display_ url":"https://www.eonline.com/news/1398427/breaking-down-beyonces-cowboy-carter-grammys-critics-and-a-nod-to-becky?cmpid=rss-syndicate-genericrss-us-t op_stories","image":"https://discover.operacdn.com/assets/tn/l/mq/3cd9

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00001c

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (24210)
Category:	dropped
Size (bytes):	24211
Entropy (8bit):	5.408789306435823
Encrypted:	false
SSDEEP:	384:dgO9rOYFAdaC/G/Fzl9A9SdP9iuFuh1ADYzHOZu1x8+tX6Q+HVqQsTx5+u9TJK2W:dgO9rOYFYhaFzl9A9SdP9jchuDY7OZuw
MD5:	F007061B725432B941E177A1C70E3A22
SHA1:	2F8F8F890F43D4CBB4021D64F11174C1DFA9BF0D
SHA-256:	6CF8F6EE951BFFFB675952645EEF32256AAB3585F62449E98FA9E3823C9503DB
SHA-512:	4EF7229D64A96FAE32B829306DB40C08D87C4E0B77FAFBB29B8BBD2D9267FB70C588B71E704CB5E6424400407424EB93792154B37666713BF7360FE975C5EE8F
Malicious:	false
Reputation:	unknown
Preview:	import{S as X,e as x,f as ee,G as z,H as y,t as u,l as m,I,R as b,Y as k,$ as U,x as $,A as w,C as Oe,a2 as O,a3 as ve,y as F,z as M,a1 as _e,L as R,M as N,a0 as v,a9 as K,af as le,aa as ie,a8 as ne,U as te,Z as Re,_ as re,ad as Ne,aq as ge,ag as $e,D as J,J as se,K as ae,aj as we,E as Ye,Q as Ze,a6 as Je,a7 as Ke,v as Ve}from"./vendor- rii-AV_I.js";import{O as fe,R as Qe,T as Xe,U as xe,V as de,X as et,c as tt,Y as He,Z as pe,_ as je,$ as It,a0 as it,a1 as Te,a2 as nt,a3 as rt,H as Se,a4 as be,a5 as st,A as at,B as ft,a6 as Ge,a7 as Ue,W as ot,a8 as ut}from"./App-CxTZVnef.js";import{B as We}from"./Badges-CuIfQk-d.js";import"./index-DtMr64Oc.js";import"./index-DQ E_taSP.js";import"./strings-D9eBrPdG.js";(function(){try{var n=typeof window<"u"?window:typeof global<"u"?global:typeof self<"u"?self:{},e=new Error().stack;e&& (n._sentryDebugIds=n._sentryDebugIds||{},n._sentryDebugIds[e]="25840fc6-f5d9-40ab-b59e-5dabb7927ecb",n._sentryDebugIdIdentifier="sentry-dbid-25840fc6-f5d9- 40ab-b59e-5dabb

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00001d	
Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	250079
Entropy (8bit):	5.379307520624104
Encrypted:	false
SSDEEP:	1536:ScanThWIBOOjer1IQOyLJbaCR6pjwSpF6JR/tJh+8Nrc0QpEWH4iLzdeKty1Raxn:DRknxj4aZQ6m2iyytgJpQszD
MD5:	35BC070C957A5BCC193C9326C1F66D59
SHA1:	4EB7DEDB0CB5216E1181D5187168C1756D407D8A
SHA-256:	7D84DE8AD5B4A038E6D81185B3796ADD562166870E94223A246ADD964FC8AA86
SHA-512:	C8B5EB549EE2DD92CB6D810903D20C018DCB96361C8935ABBF219DB0C330793DD4EA790E2141E678E996AD94E38B2193DF7FC3CD4DA3A1E69A9BE517B23A8C6D
Malicious:	false
Reputation:	unknown
Preview:	{"data":{"id":1,"key":"gx-corner-release-calendar","sectionType":[{"__component":"sections.calendar-section","id":3,"games":[{"id":400,"url":null,"hideCta":false,"release":"2024-03-09T00:00:00.000Z","hotGame":false,"onlyMobile":false,"platforms":[],"cta":{"id":35,"label":"On Steam","locale":"en","localizations":[]},"ctaExpired":null,"tag":{"id":16,"name":"DEMO","color":"#0a9574"},"game":{"id":1284,"title":"United Penguin Kingdom","website":"https://store.steampowered.com/app/2635350/United_Penguin_Kingdom/","imageOrigin":"https://www.igdb.com/games/united-penguin-kingdom","releaseDate":"2024-03-09T00:00:00.000Z","genres":[{"id":25,"name":"Strategy","localizations":[]},{"id":176,"name":"City Builder","localizations":[]},{"id":26,"name":"Survival","localizations":[]}],"platforms":[{"id":9,"name":"Windows","icon":{"id":123,"url":"https://proxy.gxcorner.games/resizer/assets/obraz_2023_08_21_154708998_8ba128313e.png"}}],"imageCoverVertical":{"id":8057,"url":"https://proxy.gxcorner.games/res

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00001e	
Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	Unicode text, UTF-8 text, with very long lines (61212), with CRLF line terminators
Category:	dropped
Size (bytes):	61309
Entropy (8bit):	5.352009200867432
Encrypted:	false
SSDEEP:	768:lxjLZeJ7PoxWPPXlBQU/VOxfeTEe3DLcQKJQSf5cqFXqf5Rm3gOYaTUYkfF:Ljo9PoxW3UckJQk5cPtSUX
MD5:	11A51F25A570C35DF4591C8CBBCC72E9
SHA1:	C2E8F0D1E72187F8A56BDE6B212A88A9CCCE6FDA
SHA-256:	5D0A9506EE0C2E64325D59451EFF05B24DF4CD07DC65F300B3BC39E28379640D
SHA-512:	1D70C0CC81A2776D7082C7C83FADBFBF3829733935CD3429CF967EB042FD0614D7048D8CA9555540986545B2C0DD2A54848CAB0C4D3081C736D52C44530AC2
Malicious:	false
Reputation:	unknown
Preview:	/* clarity-js v0.7.26: https://github.com/microsoft/clarity (License: MIT) */..!function(){"use strict";var t=Object.freeze({__proto__:null,get queue(){return Ya},get start(){return Xa},get stop(){return qa},get track(){return La}}),e=Object.freeze({__proto__:null,get clone(){return sr},get compute(){return lr},get data(){return er},get keys(){return nr},get reset(){return dr},get start(){return ur},get stop(){return hr},get trigger(){return cr},get update(){return fr}}),n=Object.freeze({__proto__:null,get check(){return yr},get compute(){return kr},get data(){return tr},get start(){return br},get stop(){return Er},get trigger(){return wr}}),a=Object.freeze({__proto__:null,get compute(){return Tr},get data(){return Or},get log(){return Mr},get reset(){return _r},get start(){return Nr},get stop(){return xr},get updates(){return Sr}}),r=Object.freeze({__proto__:null,get callbacks(){return Cr},get clear(){return Wr},get consent(){return Hr},get data(){return Ir},get electron(){return Dr},

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00001f	
Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	85951
Entropy (8bit):	5.34135523647441
Encrypted:	false
SSDEEP:	1536:fCs9gl/TkfV0Wi3imf5lfEVuTG3V5j9RN:fC4rq0WsimxlfElGFpN
MD5:	3B7EE2FE66631C3DEE312B48C763C114
SHA1:	FBD683F762D126BEF07CAB7D9665EE900B060ABB
SHA-256:	E5EF74BBB1D4467D506D261D2C94195AAC068A4BBA9877DDAA38245A523F2B4D
SHA-512:	D4EE53747DEA46057D78E9590ADBABB5B8E1837C0A0DF804DB95C126FC93DE3A651DC9AD901150940CCDD1462DDECA1F5F98EE28B30E31869AFB5582AC1324A8
Malicious:	false
Reputation:	unknown

Preview:	[{"url":"https://www.blacknut.com/en/game/62d66fa9dda24019a4b01c55_248-scribble?source=operagx&ae=23","name":"248 Scribble"},{"url":"https://www.blacknut.com/en/game/6241cd00dda24073602eaf2f_7-years-from-now?source=operagx&ae=23","name":"7 Years From Now"},{"url":"https://www.blacknut.com/en/game/591b1593b25b233ecbcbeb5c_a-new-beginning?source=operagx&ae=23","name":"A New Beginning"},{"url":"https://www.blacknut.com/en/game/5e4e9f99dda2403b883067f1_aer-memories-of-old?source=operagx&ae=23","name":"AER: Memories of Old"},{"url":"https://www.blacknut.com/en/game/60461dd4dda2400c8a96b5e3_ao-tennis-2?source=operagx&ae=23","name":"AO Tennis 2"},{"url":"https://www.blacknut.com/en/game/5d09e919dda24001ea09836c_atv-drift-tricks?source=operagx&ae=23","name":"ATV Drift & tricks"},{"url":"https://www.blacknut.com/en/game/607e858cdda2405d3b364da2_avicii-invector?source=operagx&ae=23","name":"AVICII Invector"},{"url":"https://www.blacknut.com/en/game/651d3ad1dda24047297d5be5_adams-venture-chronicl

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000020

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (32781)
Category:	dropped
Size (bytes):	33546
Entropy (8bit):	5.613741545231076
Encrypted:	false
SSDEEP:	768:oBnYvZRsmp8mpQ8smpvKAsTNbHesAmuZdRRH6zq5XfBxcvy+qMyJXolSJsTLChjO:KuRsPVqjmHs5OvYsJ
MD5:	EE8BBABEAD7DE4DEB8FD2F4ED07174A4
SHA1:	4BCA2801EAC65C92127B0BE33EFFB51852556B49
SHA-256:	E5EB44CCA16322D4135FAD351AE8C14158B6F99F866E026F625BE133013DEE23
SHA-512:	E8EA7CB96B627F2482555D5CB14A8D8619240C98A25643E06BCFDA6287BF8EFCD545686147AD011BD5BC42F11B454DC4F223D118BA7AD38BA6A66870624AC2B
Malicious:	false
Reputation:	unknown
Preview:	function __vite__mapDeps(indexes) {. if (!__vite__mapDeps.viteFileDeps) {. __vite__mapDeps.viteFileDeps = ["assets/DailyMeme-DGIR51QW.js","assets/vendor-riiAV_l.js","assets/App-CxTZVnef.js","assets/index-DtMr64Oc.js","assets/index-BRRDBs1E.css","assets/index-DQE_taSP.js","assets/strings-D9eBrPdG.js","assets/App-BVVRbkhP.css","assets/IntersectionObserver-DZG7XBCV.js","assets/DailyLayout-AjTNEUzw.js","assets/DailyLayout-DZ7n9sk7.css","assets/DailyMeme-ZC_nGymJ.css","assets/DailyRegularContent-BuVjgopR.js","assets/DailyRegularContent-D3u5Anw2.css","assets/DailyThisOrThat-vIwCIK_H.js","assets/DailyThisOrThat-DtAGpqOL.css","assets/DailyShort-CQvRSm-o.js","assets/DailyShort-B995v0Zn.css"]. }. return indexes.map((i) => __vite__mapDeps.viteFileDeps[i]).}.import{_ as ce}from"./index-DtMr64Oc.js";import{S as ne,e as se,f as ie,R as B,Y as r,aw as we,$ as M,x as j,a0 as m,N as V,A as W,aJ as b,G as A,a3 as N,H as F,U as ue,t as I,l as Z,I as P,a1 as We,v as Ee,O as Je,ab as de,a2 as Y,L as

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000021

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	18924
Entropy (8bit):	7.954790926183394
Encrypted:	false
SSDEEP:	384:F170w3ojYf5Bs7mS5huVWj/gvFc8yW+mJ4Euj845+CoXlxgzlMM7tU:Fh+6SGkjlvFJJROo1IH7m
MD5:	D701791C2DE6331066B549DB1FDE5C8B
SHA1:	4830E44DCC36218AE04FEE4D146E33BC0B5A47EE
SHA-256:	B67238C92A11972806C94AB137878CBC1B377618435CAF8FEEC6537FB71398F8
SHA-512:	226217FD4F1941FB60EA52672C4DB0E692AC0EA92A57A6B78ADEB66C0883186A39EC547AA8D31D8D2511614889389158D5C8F4CC58A5A8189AA12771572E215
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....'"%#""#-(-(/.(20----5=PB58K9--EaEKSV[][2AemdXlPY[W.....0..0W??7?WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW.....h....".....J.....!1A.Qaq."......2R....#B...3Sbr...$Cs..45c%D.....(.....!1QA."a2BR..q.....?...!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... .!...B.B.... ...z.j?.(~g~.....Mq...xs.]...O.G.;...u.....Uw..[j~...C.:.....(..i...g~.....<..}.....3.J>..}.?..7..6...t_cm>.....~..w.M.~...s.]...O.G.;.....?..7..6...!tN.6..&....g.v...@N....h.e\Z.....V..P...).....9...mH....AC..EF.6..?..p"..H}..{..3.J.....B.>...?...b._.....S...n^...I.&..J?...bm_....S...n^...K."......(..j...g~.....4..}..{..3.J>.Z..G.;...?F.9....U....3.J>.Z..G.;...?F.9....U.....S.z.jq.R..s..J....a

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000022

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	34151
Entropy (8bit):	7.971067697267996
Encrypted:	false
SSDEEP:	768:PnRSvYTKiPvA/58ilkKNVcWAtF5NXB8HjtN1kM9YV4y7Hdh8OmpVcgZtf:vRvKi3A/GiIZNVchiHlhtOkj5
MD5:	49E2B0B62F33284F880EA80E0BE89D70
SHA1:	2C698166770094 96A8CDF29EFFFEB8E5AC328F32
SHA-256:	6F0C03BE954907FEF1AEAAA50F1B64A42B31066FC69B8366B843343E81666DED
SHA-512:	E0C7FE7825671DDE9DCE6313B2C46655574E24FF3CD72BA4C84C1BC74F817DB5E3BFEEC1E39480779AC3C1AA1BF9898A577F6030364759AC7FBE8280491291C

Malicious:	false
Reputation:	unknown
Preview:	......JFIF...h...."...R.........................!1.AQ.."a.2q....B. ....#RSbr...3...CT...$.....Dt...cs...d...............................9........................!1AQa..q..."2....BR.......#b%5S............?...Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@ ..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@ ..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..'.x+.sm...$."DJ..:.=..t..5..m..!.U.....".bi.w.J...TU..z>.p.G..`.g.z. ...N...}..d...%.............(.qv(]..s.....j*....z.l.le.,.7..-..eJ..G."E...~........W..]^...ygQ&s.+....W.,.......a}.....p..j.u;....q.}..[.......U..(..}..?m..e.....3...d..+m.g.w+.....e...h...z...'l.........h....`x... {.z?....\7./.OM.5..k#.........._..................2....._....a.z9-......\7

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000023

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	31169
Entropy (8bit):	7.965196413015818
Encrypted:	false
SSDEEP:	768:ubeuvXBR3r1KzEFJ3JxDw5HZ0l+8jyesyve:Oe2XB55xDQ0/syve
MD5:	B3C143B38FF236A7AD6F053494B1E177
SHA1:	ECCEECF97B614FE461C19315BAB233D7A41DCE8B
SHA-256:	9DDED002A0B068C4072F96C6A615BF0A77CE2DB3390103C1DA8EC5E8017ED660
SHA-512:	E92BAFFD7747A6C811D7121CDB4C7B9B0C26A529034C2E535F76C5E4A6A8764613B21375F301FCE41EF2988D40C0EBBECC2245527C61C1B6E739E65C93B3B3 1
Malicious:	false
Reputation:	unknown
Preview:	......JFIF...h...."...c.........................!.1.."AQa.2q...#R ..Bbr.......3CTUV..........$Scs...%45....Dtu...6EF....'................................<........................!1..AQaq.."2........BR..#b..$%r..............?..TQE.QE..E.P..Q@.QE.QE..E.P..Q @.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE. QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E.P..Q@.QE.QE..E{j.(............4.4VA+..M.....5.R|.f.j.......S+".+p./....[$...M..@\|....9R.3#U......{.4.... ..e[.>.fG5..Sx....en\...>'..r'...%QJO.8._......w=..?...=N..+..E,....'...C'..O.5>.W.Y......o..<W...W...O......W.Y<...(.y8~A.....i9;.....e=.....q:..z3.S......T...Y.ek.V...pV.;..j..G...{Q.,d..@ .$c..ll..2"...'...x...5. b.&....T.....T...

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000024

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	Unicode text, UTF-8 text, with very long lines (65529), with no line terminators
Category:	dropped
Size (bytes):	104392
Entropy (8bit):	5.447610322095709
Encrypted:	false
SSDEEP:	1536:BkDEh3IM8XxGhahyVVoKHEZLs9ccKO4AreJsHxCpSU/GD7a7f1dUWXFFS:BkfxGAUVNEZbIHxC4om7a79GazS
MD5:	78D89D9CC064FB0A09530DA2C00DD81E
SHA1:	12E95DFCB58AEF646C8EA70C73FE506B0FF2982F
SHA-256:	10B7A6A70DD63473878E033A88A12AC3B6D3C49191FE0CA8E3F2BAFD96B80B4C
SHA-512:	F888CD2AE12370C6ABA517F0AF32378BC9F5C11E07A21C440971B471822533A30BB2C05C4555EA5BD99531236E9A47A01445A229A2B912ADE5BC9FC91447BA6
Malicious:	false
Reputation:	unknown
Preview:	import{S as ve,e as Me,f as Ce,a2 as Y,R as O,L as he,Y as N,$ as R,x as D,a0 as w,U as z,ai as re,Z as rt,M as Pe,_ as jt,N as me,A as F,ad as ut,C as Je,aq as bt,n as di,aF as po,aJ as Xe,h as se,D as mo,T as An,ao as bn,t as S,y as oe,l as C,z as ae,u as le,j as ce,k as ue,J as go,aK as ho,O as yo,aL as Ao,o as bo,am as xe,v as xt,G as fe,H as de,I as pe,a1 as Ge,Q as ke,ab as Nt,ac as pi,a6 as st,a3 as te,a7 as lt,a9 as qt,af as je}from"./vendor-rii-AV_l.js";import{t as qe,u as No,v as Nn,x as _n,y as Sn,z as En,A as _o,D as So,E as Eo,I as vo,k as Mo,F as Zt,l as Co,B as wo,G as yt,H as vn}from"./App-CxTZVnef.js";import{c as Io,g as To,a as Mn,t as ko,o as Yt,b as Cn}from"./time-ewJhiJwX.js";import"./index-DtMr64Oc.js";import"./index-DQE_taSP.js";import"./strings-D9eBrPdG.js";(function(){try{var e=typeof window<"u"?window:t ypeof global<"u"?global:typeof self<"u"?self:{},t=new Error().stack;t&&(e._sentryDebugIds=e._sentryDebugIds||{},e._sentryDebugIds[t]="8da8aeb6-e95d-4377-8abc-e1

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000025

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	28885
Entropy (8bit):	7.940251079924301
Encrypted:	false
SSDEEP:	384:mOrvnDZbCY946AyYurYMexwt+Kxn52Ww60YKfUGkzUDQCvpmK+6OXcTRXU9C8ZoE:9vF+YdreI+Kxn5RwDuGwGjLAUXUkMoE
MD5:	6909E84F1F144505D2376D14F66DE5C9
SHA1:	97A2389BD1BEF3D7A76B8D23A305696C38F8D5BF
SHA-256:	83A688ADF108B5F9FB16F2630E7B20A826A6572461A280F9FA029B38E733E5DE

SHA-512:	BD0EE0BA70AE482042593824CB7EE1425E3687F6BC60237E48D92AA8E60555E5272A20A2A4F6D7990C91B6354EB9402285618DBCC469CDA8FD2C85265D2AC7E F
Malicious:	false
Reputation:	unknown
Preview:	......JFIF...h...."..O......................!..1AQ."aq......2BR.. ...#r...3bs...S.....$C........DTc................................3........................!1Q.A..a."q...2...$...Rbr...........?.... ... ...,..x.....{..5..fG...(.....}L.<~Pd..Dh"G...=.}P....&|.$G.%}D.<~P.d<<.A.>..#...X......=.....!.!... ..}T....T..Hb.\|..=..PxA...........Y..d.r.1!.!.g<!=I..\.....T`...%.]...}\..:....p.CPC.W<#.e<<.B....b..,gQ....{...\..$@.,....{...vR.Oy.A.... A..d.T...(lu......H..-S..sGy....>.Q..,.r.1........;..ai...i.. ..e..8#@:%7........}.}...e.fG.;.i.Cg{R...!i.L.jW.W..\.dy3.F...

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000026

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (45271)
Category:	dropped
Size (bytes):	308035
Entropy (8bit):	5.318298420291545
Encrypted:	false
SSDEEP:	3072:59pX0oT0xaIrfHTfSWfHBgwvmPfSiGvjclyGnrSTc+yPnsTS2hEKzwuDPIh:XpaxaIrHjS8HBgCm37GhsO2hBwM4
MD5:	AC954F713DB49D6EBB0BD8AB9E89CEEB
SHA1:	54FDEE88EB04124B05B14C17F491A688A838E5D1
SHA-256:	D0B68B4ED4564D03B8A90CAC1F94FCD46CE0F3D702973D305C0E517B1A0772DC
SHA-512:	6696CFA5A9CF8A764D2C294E1AD69DF2B03C4826D8862024EA373C101592B738FE54FC9188BA23E11C91EED8C3FB3CB95D83A6C484AC42F24EBE77C3EDA48 BE
Malicious:	false
Reputation:	unknown
Preview:	import{V as getDefaultExportFromCjs,aD as commonjsGlobal}from"./vendor-rii-AV_l.js";(function(){try{var t=typeof window<"u"?window:typeof global<"u"?global:typeof self<"u"?self:{},e=new Error().stack;e&&(t._sentryDebugIds=t._sentryDebugIds||{},t._sentryDebugIds[e]="d6bc7e12-fe38-4f1d-9e8f-8703ec599f58",t._sentryDebugIdIdentifier="sentry-dbid-d6bc7e12-fe38-4f1d-9e8f-8703ec599f58")}catch{}})();function _mergeNamespaces(t,e){for(var r=0;r<e.length;r++){const i=e[r];if(typeof i!="string"&&!Array.isArray(i)){for(const s in i)if(s!=="default"&&!(s in t)){const a=Object.getOwnPropertyDescriptor(i,s);a&&Object.defineProperty(t,s,a.get?a:{enumerable:!0,get:()=>i[s]})}}}return Object.freeze(Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}))}var lottie$2={exports:{}};(function(module,exports){typeof navigator<"u"&&function(t,e){module.exports=e()}(commonjsGlobal,function(){var svgNS="http://www.w3.org/2000/svg",locationHref="",_useWebWorker=!1,initialDefaultFrame=-999999,setWebWorker=f

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000027

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	46382
Entropy (8bit):	7.982149997883431
Encrypted:	false
SSDEEP:	768:gHzZJ2SLD6MdfOlYtW60WRpFQ/poWnamhPANn3fIP2u3g2ngIfx1BS0at85xHxRq:CJJVdNtG6G/G04nPwhw2jfstCxHxRbE3
MD5:	3FD8293AD6D39E4DAAFFB3E57D379B57
SHA1:	FCEB352704BE7F86E1730830896BEF5C758A28F4
SHA-256:	EBAD314AC5ED0B58ABF73CA816067A35B8B6CA3356B6E7CCF62B83F4448A6CC5
SHA-512:	7E37166764DAF506A3D707394648B71A87917C7410F713EBFE5D388859A9DB8EC7B8EF584649C94B46E707D2B02FC158389F87DA9F0F1C4F0FAADDD6EEB91A4 A
Malicious:	false
Reputation:	unknown
Preview:	......JFIF...h...."..a.........................!.1..."AQa.2q.#... BR.......$3Cbrt......45STUsu....%&Dcd.....6E....e....................................G......................!..1.AQ."aq.......2R....#3Bbr..4..$Cc.....Sd..............?..X0`..`........F..0!.0`..`........F..0!. 0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`........F..0!.0`..`...... ..F..0!.0`..`........F..0!.0.z8.k....t]...........9.0a}.)'.}m.\s.:>......!Fp.0aE.C]Z...........8...E....4+.s..B...ad.q...?.....Y......G....>.k....K#.i.u....Z.5.....t..m5.6......./.7.1......S.S...W..o....;...../ .?.1.uu?...... .j.0..)...1....}......ng......f...Ll.I.3pa.:....S..g...W.<...?.x.......W.S.

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000028

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	55728
Entropy (8bit):	7.98248543718097
Encrypted:	false
SSDEEP:	1536:3cW13tnyk6xJH65qJpua+WYMjkHQzRJkPU0Hkzmtl:33tnkfa0zuq4Q2Mmtl
MD5:	F4F5A7C0DC5A255EED4473DBEE6EF825
SHA1:	75E6C24FE94DFC9DC4CE014E7D266E3BC96BBA18

SHA-256:	2C26AA04D0C2EAE9F1799E125C561626DCDFE881B0339F7AAEDB7AF45500F832
SHA-512:	E029FDD6491BD12DBE4C1D053682582962F895880ADC6012A257BF7CAB38E78B71B0230796E9107B58714A79283E013CE88279D4409B0722D08F0117D3037D8F
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....h...."...`.....!..1.."AQ.2aq.#B.. R....$3br.....%CSt....5DTUs...4d....c....Eeu.....J.....!1AQa..q"2.....BR.#br.....3CSs.....T..$4c.....?...,.0`B0`.....#.....0`B0`.....#... ...0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.... ..0`B0`.....#.....0`B0`.....#.....q^H.3L.....eF.w..<|%.G.P.....{i.....F.Q.10yzOT.O.q.r.....(.....S.WC.k.....+#..VC..n.MC.r..'.|.....}nZ..?..4.....R.....-.;.s.XM..<.5..5.,|. m...N<g92U j....G..^.[F...O..Wr...I.X15'-.<..?...!...'.....I..co.....w4.....Jp:77p.bx.pbf^\.m`..(s[]XJ..

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_000029

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	48982
Entropy (8bit):	7.980351047693944
Encrypted:	false
SSDEEP:	768:tcakHPtSz0nGUw1wKzaRrC6+65nG/7j6B76gkldYNZra6MfONNE14PBNHwUU2:tYvcoGqKQrr+MGyNk+lv4PBJwUd
MD5:	3720F60FEDD41C793BAE75824F74F5EC
SHA1:	B239356B6DC3B63065E87083E07A0DD92395C9A3
SHA-256:	B0D6B083A1D6E9AB4EB7C6B5F98C8BBECB3B6F806C44A9C782D2E0F46741617A
SHA-512:	042B72121DD20162277ACCAB4FABA72FABE90587C4446F8021492C96FBC734969161C3441DB70293EB737C51C023FB7C61702267651C4AD676FD4A10FE3C457
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....h...."...b.....!..1..."AQ2aq....#B R.br.....$3t.....%45CScs.....DTu..EUde.....&6.....?.....!1.AQa."q.....2....#BRr.....3...Ss.$.....?...,.0`B0`.....#.....0`B0`.....#.....0`B0`.. .....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`.....#.....0`B0`... ....#.....0`B0`.....#.....{..g...../q...?.....5.....L.....I..|co.V..nS.$..1!....;:.j..0..&..j.eH.6.nuu.....G..$.&."Q.....W..].>...I'.....5.!....|.3.I..../.DcV..S4.....WU..>4..E: ...aY...Mky/.h..L*.s..30.\U"a..0.....r.....3..U.2..G...(.A.5.[.W=.....P.b`tu..v4w<...x.....Y./.

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00002a

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text, with very long lines (59000)
Category:	dropped
Size (bytes):	149994
Entropy (8bit):	4.84602990632708
Encrypted:	false
SSDEEP:	1536:1kV7f/AI/gc0w1aQie8IMVxbFg2W20UfTR+rLrg:CS0w1aQKVxbFD0UbR+rvg
MD5:	F6C5A55CEE02422E137B999BF80B410B
SHA1:	EF9EDF54FFD0656A5B86582CC737FDDB834CF2C5
SHA-256:	99FB52370E2691FF26A51DE772CEBE42DED1C9189312035C518F9EF185BC7EDE
SHA-512:	24ED70A60D3BB8B4CCBACA8EF6F070C7070D20218E62D7B4DDDE563EBD227AF08771C77E1FE5B9C011448EBA1EE947F77BB642E72432E80D659C07F35059DF 55
Malicious:	false
Reputation:	unknown
Preview:	/*@cc_on;document.querySelectorAll||(document.querySelectorAll=function(e){var c,t=document.createElement('style'),i=[];for(document.documentElement.firstChild. appendChild(t),document._qsa=[],t.styleSheet.cssText=e+'{x-qsa:expression(document._qsa && document._qsa.push(this))}',window.scrollBy(0,0),t.parentNode.removeC hild(t);document._qsa.length;)(c=document._qsa.shift()).style.removeAttribute('x-qsa'),i.push(c);return document._qsa=null,i}),document.querySelector||(document .querySelector=function(e){var t=document.querySelectorAll(e);return t.length?t[0]:null});@*/ !(function () {. var t = function (e) {. return e.replace(/^\s+|\s+$/g, "");. },. c = function (e) {. return new RegExp("(^\|\\s+)" + e + "(\\s+\|$)");. },. i = function (e, t, c) {. for (var i = 0; i < e.length; i++) t.call(c, e[i]);. };. function e(e) {. this.element = e;. }. (e.prototype = {. add: function () {. i(. arguments,. function (e) {. this.contai

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\f_00002b

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	168929
Entropy (8bit):	4.007094560453527
Encrypted:	false
SSDEEP:	1536:abYq5nbbUb42qHrbQbbDFbubAjCbwb7bHb/bXbumbeIb1b4bbbybVbRb1bJ/F2sT:r/HHAsY9Bj2
MD5:	C9CAA63A244892710CC32810566B4285
SHA1:	89222142B1083369A27B2B76710D7C78044A4D68
SHA-256:	0560FE562F97D895A6E265D17BC3B9C53DA8D9F8FABCFFD4AB5C0662B1D3534F

SHA-512:	6C5C949A524CBF19F7B990870833EE8F257F4024B6638C86740351CDC828C5B5ED687F4C51771E652EE900D6843DBEB0B20D975847935347C1E648955DCFFDF9
Malicious:	false
Reputation:	unknown
Preview:	!(function (e) {. var t = {};. function n(r) {. if (t[r]) return t[r].exports;. var o = (t[r] = { i: r, l: !1, exports: {} });. return e[r].call(o.exports, o, o.exports, n), (o.l = !0), o.e xports;. }. (n.m = e),. (n.c = t),. (n.d = function (e, t, r) {. n.o(e, t) || Object.defineProperty(e, t, { enumerable: !0, get: r });. }),. (n.r = function (e) {. "undefined" != typeof Symbol &&. Symbol.toStringTag &&. Object.defineProperty(e, Symbol.toStringTag, { value: "Module" }),. Object.defineProperty(e, "__esModule", { value: !0 });. }),. (n.t = function (e, t) {. if ((1 & t && (e = n(e)), 8 & t)) return e;. if (4 & t && "object" == typeof e && e && e.__esModule) return e;. var r = Object.create(null);. if (. (n.r(r),. Object.defineProperty(r, "default", { enumerable: !0, value: e }),. 2 & t && "string" != typeof e).). for (var o in e). n.d(. r,. o

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\Cache\Cache_Data\index

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	FoxPro FPT, blocks size 768, next free block index 3284796353, field type 0
Category:	dropped
Size (bytes):	524656
Entropy (8bit):	5.027445846313988E-4
Encrypted:	false
SSDEEP:	3:Lsul7Q:LsR
MD5:	29E8EA0D6F9D7B5FA89C72516588280A
SHA1:	77C5168025DF5F09C21050AAB42CCC550C91B6D6
SHA-256:	1ECA1C6E80787DA4E7E75D48B868A7F535B0D06A07A470B85C086BA8CAF51C89
SHA-512:	2FCCF4014891CA334222FDC591F2D0684FF9BA8EFF3094685EF8A5798CE632294C856D993395D77B97159FFDDEC70689CA3D7B8D0093F6E306E658BABB993AC
Malicious:	false
Reputation:	unknown
Preview:	.....dU..fs/..... ....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\System Cache\Cache_Data\data_0

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.04469063214076828
Encrypted:	false
SSDEEP:	6:/Fii23PKkN+HPuqTbZiRPTrh9S6fkJl7Q37S8Mtk1:d+/NOmxPfh9xMJ637vEU
MD5:	D0753BA8F9AC14BFC8E9115C76D17D67
SHA1:	1E3739F2CB63A353BDDD97989086E162EEF674B0
SHA-256:	A78B62318268283C3C801E8C759AB3727BA5769C6BC23AAA9F3647D60C5EE585
SHA-512:	449C942F1DE8C13311537146AFA0F1AB7837812E2B8F52D7BF3B9406077260119688D931FBE9ECFB1590D49A25EDA6B73C302A451B5823E96EEE3DD96E2FE7D A
Malicious:	false
Reputation:	unknown
Preview:	.....$..... ....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\System Cache\Cache_Data\data_1

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.05722599312702698
Encrypted:	false
SSDEEP:	48:UwSwcL/kfwSwc2i5iM9g0zbr6ei5iMj8g:UVJyVYi5iMlzbOei5iM
MD5:	595F44D4E26401BD49DADAC8B2BCF35B
SHA1:	10344E8FC3A9CA736CC259B2F213A21A00BFE620
SHA-256:	296CD2B453A48D2EECD08644F29549B588E539C75380C1F728767E7A1D29F29D
SHA-512:	44CA9E78F85E351DAE53A9FD11C3279809DFEB9A2BAB3A71B3D29ACB849E26BA09FDFC9096E5C31852E83AACBDF867A2393469951503727320F4C4999D3B39A 4
Malicious:	false

Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\System Cache\Cache_Data\data_2

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	1056768
Entropy (8bit):	0.278164822408153
Encrypted:	false
SSDEEP:	384:ztLqXJtITaRvAGIEC418gqXJtIdkXRJtCiWfUPIALKJtrLCXRJtC:pLqXJtYa13qXJtnXRJt+cPIBJtyXRJt
MD5:	AB2BBE05B5835E7D99546FC2D02529B7
SHA1:	81517920C3F78957346C1504A5B9DE825D6C9ED8
SHA-256:	DC9BB94AB3D191E9327D3B81D27A53DEF3F7D86805D0E5C82666FB1F4A89ACFB
SHA-512:	BDA8EC83FBB5374FA5664CB2767EC83514CA6FA794917ED7702AAA4BA6A9CC9609D188EDC6F6A60CBC6FBAB484AE8CA8883B898D91BDB75FEF744DE30598525D
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\System Cache\Cache_Data\data_3

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.012340643231932763
Encrypted:	false
SSDEEP:	3:MsGl3ll:/y
MD5:	41876349CB12D6DB992F1309F22DF3F0
SHA1:	5CF26B3420FC0302CD0A71E8D029739B8765BE27
SHA-256:	E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C
SHA-512:	E9A4FC1F7CB6AE2901F8E02354A92C4AAA7A53C640DCF692DB42A27A5ACC2A3BFB25A0DE0EB08AB53983132016E7D43132EA4292E439BB636AAFD53FB6EF907E
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\System Cache\Cache_Data\f_000001

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	140775
Entropy (8bit):	5.170244966514947
Encrypted:	false
SSDEEP:	1536:Jp3CD0SMi6We1mJXDDRmrAe4xnzR7vvODy:JpSM3We4JTXz9WDy
MD5:	1EF34DCFC08237E317B9EA5E6494D429
SHA1:	1929EE76DC7603F9F7527ED3370C2723E507714A
SHA-256:	07A35BE742E8543E4918EEE6D95068A77E146874BFB0EB8D60904D761C06A9D0
SHA-512:	1039DB8A6E2D1EF175B13F57AE585E33575F450E9EA9036D03D2516F1071127175E2C34B9D3D08B71445C87FCCE2DE40FDD23E23FAE3181B552020E6B82E52B
Malicious:	false
Reputation:	unknown

Preview:	{"suggestions": [{"name": "Humble Bundle", "partner_id": "gx_humblebundle_suggestions", "url": "https://www.humblebundle.com/", "thumbnail_url": "https://sd-images.operacdn.com/api/v1/images/422e375ff749adde024ab3ea5ea01275e40e5f1b.png", "history_patterns": [], "priority": 0, "favicon_url": "https://sd-images.operacdn.com/api/v1/images/ad4ac5dd18b5c44cdc22a37217bfec19a3abebd1.png", "real_url": "https://www.tkqlhce.com/click-8384705-14473383?sid=operagx-desktop-global", "ping_url": "https://speeddials.opera.com/api/v2/ping/gx_humblebundle_suggestions", "keywords": [], "categories": [], "rank": 1, "targeted": true, "ignore_sd_filter": true, "required_dna": [], "forbidden_dna": []}, {"name": "Fanatical", "partner_id": "gx_fanatical_suggestions", "url": "https://www.fanatical.com", "thumbnail_url": "https://sd-images.operacdn.com/api/v1/images/4335dc32a6e411f84f57cd66d91181c53788d707.png", "history_patterns": [], "priority": 0, "favicon_url": "https://sd-images.operacdn.com/api/v1/images/d

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\System Cache\Cache_Data\f_000002

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	541788
Entropy (8bit):	5.186042707102053
Encrypted:	false
SSDEEP:	3072:JpSM3We4JTWdslsQeTOrT2lNbesv0lfTv7029UZz1cFxeg9i/RAimqs1:JpR3W5JTUnfNbes8t029sz1cl/RAiRk
MD5:	675383AD7E1EF3C02E7DF37DF0FC2D41
SHA1:	B91A68A5C89DC24D238FF1D75CA3E7CFAA0515DB
SHA-256:	756FE8D8D1D3C0E6E0E027475A713F30465A3FCF32F860CBD7F3BCCBB7648BC5
SHA-512:	88ED4970C3D5E1824A18AF9FC0F749C9F1D46EE98422E285BDFDB9B0CFDEFAAFC286425C25CBF0F716B043078583B1BEDFB2FD3C094919EC0AB572573A18E32F
Malicious:	false
Reputation:	unknown
Preview:	{"suggestions": [{"name": "Humble Bundle", "partner_id": "gx_humblebundle_suggestions", "url": "https://www.humblebundle.com/", "thumbnail_url": "https://sd-images.operacdn.com/api/v1/images/422e375ff749adde024ab3ea5ea01275e40e5f1b.png", "history_patterns": [], "priority": 0, "favicon_url": "https://sd-images.operacdn.com/api/v1/images/ad4ac5dd18b5c44cdc22a37217bfec19a3abebd1.png", "real_url": "https://www.tkqlhce.com/click-8384705-14473383?sid=operagx-desktop-global", "ping_url": "https://speeddials.opera.com/api/v2/ping/gx_humblebundle_suggestions", "keywords": [], "categories": [], "rank": 1, "targeted": true, "ignore_sd_filter": true, "required_dna": [], "forbidden_dna": []}, {"name": "Fanatical", "partner_id": "gx_fanatical_suggestions", "url": "https://www.fanatical.com", "thumbnail_url": "https://sd-images.operacdn.com/api/v1/images/4335dc32a6e411f84f57cd66d91181c53788d707.png", "history_patterns": [], "priority": 0, "favicon_url": "https://sd-images.operacdn.com/api/v1/images/d

C:\Users\user\AppData\Local\Opera Software\Opera GX Stable\System Cache\Cache_Data\index

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
File Type:	FoxPro FPT, blocks size 768, next free block index 3284796353, field type 0
Category:	dropped
Size (bytes):	524656
Entropy (8bit):	5.027445846313988E-4
Encrypted:	false
SSDEEP:	3:Lsul8cD3/:LsU7
MD5:	7A243265D23345D318FB436CD1B6C04B
SHA1:	B69638F8C981344078B312DC6FC8E3A499301A9F
SHA-256:	0140C530E78C89C13CEB89B964A57C125A8A935A45D2424819D640DA6D170084
SHA-512:	185492621AFD90C1E95B2C1B4339C6DD4D68EFB82FF4BA707E3E22FF988AAF1CE3E5706658D99A5EA690DE9BE0958BCFB100C3A552BDC2A7D4455AA7777AB419
Malicious:	false
Reputation:	unknown
Preview:	.....qa.fs/..... ....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\107.0.5045.79.manifest

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	225
Entropy (8bit):	4.929804541487484
Encrypted:	false
SSDEEP:	6:KdhlRu9TbX+A8/5RFYpThkokIkoX0CdiYCWoA1G:KLuVA5cp1kvIks07vWBG
MD5:	C45BDB4215269232365A5939FDCFD5EF
SHA1:	6947C09E83ED9FF44C747280104CE62C129CE08B
SHA-256:	881561A1AF511D35898655D5233605380EF1E71111781C05F637AE7EC578B216
SHA-512:	0575A827C9C57FD1B7EDA4FDC6B5D710EE87AB3CCB1F74CF3F3E6A771A1EFCE490F549BF90803D237352D6E461E3275EA90B9D41B701E56F8DBFD07F44733E14

Malicious:	false
Reputation:	unknown
Preview:	<assembly.. xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>.. <assemblyIdentity.. name='107.0.5045.79'.. version='107.0.5045.79'.. type='win32'/>.. <file name='opera_elf.dll'/>..</assembly>..

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-100.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2181
Entropy (8bit):	7.807674908350133
Encrypted:	false
SSDEEP:	48:Pe+1prHq0WWdnFX5lKhqEiJVk10s5pqe/cme:G+1prHqXkhrWqEiJa10ae
MD5:	B5A21B88B3D8A42DF265817EBEB742BB
SHA1:	E0BE32B4FC158DB4E9783094CCE614922114B742
SHA-256:	9635C074C9D8EDDE0BAF3111DBD7DB49CBDC370C4F729C80AC382949F32BE526
SHA-512:	21ECE0DCF17B038400D09565438FCE8BE61746DAA0250F2FA9D0526BBA3D1CE6F8DA5CCE944EF8FA685C5EB6CF857B073D2A50ADA44A44A76D84813871FAA D0
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....<.q....LIDATx...1..... ..6.^`.....{.....m.m].m.m.m.....[s....._.....N.Nw..._w..P...R... .....`....._[.i1...`.$.....C.....*.,...v.l.>.ZP.B...E@.....!?d.. !.d.R.....g)0...^H[.u.4.k`....0<.d.1.....0...Q`..I.._T..!...|pG.m=..a&.e.U(...C...n.^`.....FB.X...Oio...z!...:.Tx.8;..9.[a.....{.~.^.....P.].r..d..A...?....<y.v".....l.....^.._.....MA.o.... ?.>u._.d..`.....E.@.5.....E.....R...A..O){.k..2.....jx\..5U.a.%."#.nA....6.!..W2.....R..j6r..v...."....N.GA..8.....>..p..#..,X.....Q...y..#.a..)....Q.e.zc\.'@.Al.....io....= .....D.....F.....A#6.^.^.Ma5...b.b...D...+.P.. .[.o..z....,...#<U.0.O.#..Z.....Q{...jA..ka|}...q.s.y^.!.Gh..R....t.g....F.....gt..6...7YjaU....0.*.....3..l.#.. =.h0t.06.v..C...T.}m..%...g ..i,Cq..8.g.q..hx. .>..Kz...1....VF.)..q..$....._Z-.U...(....~>...-z]$.mh.%...e.+.....|.n.2..:...N._R..x..>.|S.....i?.P....Q.F.d..U.8..i...T.....I.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-100_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 150 x 150, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	1828
Entropy (8bit):	7.716814612583543
Encrypted:	false
SSDEEP:	48:uIrxqF+qFL9yUaKagPWex0mLgIbPdyFKD0YTkogFey6mkAN7G:3wFRoGagTx0A4KDfTko6eCZG
MD5:	0BAE0648C3E320C4D439F158B4FD5531
SHA1:	4E860AE24F03522C89BDF37F3CCC10B54832861E
SHA-256:	28CE8FCB22080CE1F69346CB0720BBE5662959E413426F00062B706013DA8C28
SHA-512:	6A5E4105CCBE1664546798DB057B93622C9CBD6D5AF4967E6BE4E390A18FEC0FFCC807E3331F09ED0DE63ED85569BE7EC5EED5A7C663DF6CE4A5B70E09500 371
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....i....IDATx...i.]U.....J..RT.H....T...seV..)b.B.5.@.a.Q..P.c. 2E....eR...P(.....P.....I...s..v...y...u.....Q.EQ.EQ.EQ.EQ.EQ.EQ.EQ...S.n...j.."....p.. |B..]....>.....9.32.....Y.I.R..*y.\.8.4.....p.K..EY%}.5.h.[*.|.V..i.F..q~...;..W61.M5_..1F...Gj..IZ..u. ...*.w....oS..D.r.).U....j.y.#..y..U..;S.-"...n..v.^i.UW.j.hk...n.....,...LRe[.i.}.. ..H.z@.9.q..".v.U9.""n.)....DD.iX.b.....*'....v5.#..~.$.7.]..Tm.....i.....+....m...x.j_.'"NG.]..n.j.vl{..Ls...;.T.=E..3...1;.v..xB...*"^.1U..8...xL,7]...D.9.i.."..N..."...c..D...X...c+.t..8M...[..... "f.....R..0R.1..Xh..;ND.=U.ID.a.....v..8...'.uct.....k.q>.q.jc.+b...F....r....AN.....}.....Y.J.k~.;4.3".U....s..$....n.q.b{.q.j.....".Y_..E...b.=.S."..4...[...S....Y.6O.L...."...."......i../"..!M. >..4ED.....I.."'60x.Ct.i...4..".f..`(.....4..5.L....o.....*W....xX.M...E..C...r.....U...8..<'.G.}D....E.k!.8...ED..iL...V.8.."b.C3[Dl..gED..^....-...NDL.iBs..O...`m..zW...k.A

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-140.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 210 x 210, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	3140
Entropy (8bit):	7.81304512495968
Encrypted:	false
SSDEEP:	96:X4+RWiQZwj2bSjtW8+i2elETWt5nQ1pzuiV8:ozEW8+iZECt9kzuie
MD5:	7E529063A02E4E83736B0263CB1B82E0
SHA1:	17A3C4B76962E90B1D2FA8A49441157949F4DC78
SHA-256:	A36A13A5D5E3D39E3018CCC5F8859944C87256F8BE24A3C08A6BF3CB06A26804
SHA-512:	571806725F83FECA90360B246D167A8857EDFD9EDC8DC0EF7EEEF80F291FD06088C405A5653513CB8AA309DF08CD609DF85A95E3379E3E5907566C876CA77CD E
Malicious:	false
Reputation:	unknown

Preview:

.PNG........IHDR.............?..B....IDATx...{..dg.8....m....m.Z.m..;;y...s.GI?..Su..k=.T#..#.;..}/\.g..:b..a+.....t.A}...q..hq.-.}...`:.gk....tm.$...Ax.....B....c.i
h....G6L.....;...T.U0...l....~...........W....=<j.....X..O.....r.Y..-..Q..1.....q`..PC..jL...x.'9........y.b=L.m..(U........a.....W......`:.Me.jh..U0.......;..{..I..|.W..C..4...b.nt.......L..a.........`9.!..7N@
.......E.?..$.._.q..6..":.+`....W.O.G>o.F.K.c..G.28..Q.....|.....m..#X......N.P..{:...1.........4...F.....w......Z89.Y.w`.L...v.DC.h'......h...[=...c.2...&ze*h..t..j...@?..cpN......0...KC.....f..F....
.2"...c1..m.)y..q..(..C,.e..!w.N@I..q4.......!.A...;q..Y..sy.{...."L.p..#<...'.-8.!u.C#...O;.......y<.=....h.c<.=...5N...s....._...p,..Ia...yo....=...Y..4...t.}m@....g._.......#.M{...t........t...;.bj
h..l..84.C8..z....B9..[.D.R..}...r..e.pl...~.....<.~ `...Ep..b...L.^.9..x.vB..IZH.a,k..c..L..U...M0....}.n........H..<.!..B.(Y

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-140_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 210 x 210, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	2659
Entropy (8bit):	7.828610258666657
Encrypted:	false
SSDEEP:	48:zQX9JrPPPPPPnouwOIlbylOhFARjcSY1E1y0fAiKb+Y+GzYvpSYWTX5sPPPPPPPn:z0rPPPPPPojFby+m00fAiKiySSYWTXqP
MD5:	EBE7D27ED3B4CB6566A10165ABFAA941
SHA1:	FDF7C27058CF5DAF7061756E938A33C1BBB26C3D
SHA-256:	0BD63FE653885286E180FBDF6D1DADC66AF242B8ED6BD1D03D8C5ECCC20E91D7
SHA-512:	50EC8592D78F00A6387F06E077E0DEF88DB26723C0FB8632C4EA06F2E09488DB0FB82E0EB1F03DA53F9C750F6CEBD29F7889B1DE342E4F0AE69F88C4B7B1425 B
Malicious:	false
Reputation:	unknown

Preview:

.PNG........IHDR..............V....*IDATx...{.]U}......"... .!.#..D .k..:.....5...6B..Q@+..lq.(%my.P..C-..Eb..<L5..<C!.1.$wu...f..}........5..Yk...^{.}..RJ)..RJ)..RJ)..RJ)..RJ)..RJ)..RJ)..R
J)u.d.Y.b?t..Q.E.,u......$o.-..rK....nw..7..w.TF..-...5=.r....?N...a.N.....~7..7,...r..-..q.}..R....Ye#y.u...IF2...Z..6.o.F....R1<w..]T..H..zw{.k..Y.L.Fm.k.ay.W.P.....I..,5G..C..........v.]...].-
R..A......1.a;J-..>E....Qe'............#^VF.J.J-.....LRe.....|....g.M.e.+<.l$gHM.l..y..T.s#.Ow.o+....=...4....P"..J...("...]...~....z...h...P.*..QD....Fg.a..7m...W.`.j..C.q...E....D........8.i..D
...^c...J.,.../.&rH[M..9.4._kfzN..#..bD.....[.D.4M3.....2Cs.........._k.Z%....bs7+...wkf...'.%..D.j..!M4A.z-R.k5.....q+-.*&j,..GE......p..(.j_V"......i.M...7.....E..LUz.8>i..jm....[.T.].F.%Q
.;.2.....X.x.....-...b...;EQ..dU...avR[..V...f....`,.....J........K...........NWe.....Z:YT.>..{....-..(.uvV......P.x...m..ku.)q..Z>9vU;.)..xTC........j"..ra..D..(..6...t.Ib.O.....D

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-180.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 270 x 270, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3904
Entropy (8bit):	7.301300867894784
Encrypted:	false
SSDEEP:	48:Fe0zdfrjvg/ofL7NkqKgOL6bq64wL3XtakhXSTxyfO8cg7WZUScsO62vSQ6Q4MCR:JdfrYoDdbJlXBRSMoj6H626Qr45eg
MD5:	F332E088E89B88070EF1EFBECA5B90F8
SHA1:	86129A8B1E2E7F78D6CE23C58A37FAC9DA5E566D
SHA-256:	6A8F64754C75EDCC9ABC1138E44ACBD7064D7E8E2A28783939241DBD6AFA30A5
SHA-512:	2314AAE692C024F914661E46CFD76531DA6C09B94C084FE915A0594625927DF30282D09518A950EAFCFDD2E499B1E4877CF3CDBF5509DE0CC756DADCDE43FD 5
Malicious:	false
Reputation:	unknown

Preview:

.PNG........IHDR.............Oo......PLTE.....N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N.
.N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N
..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..
N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N.
.N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N..N...*....tRNS..8Uq...........jO+..D......o3.0y..b...g..a...@.....
..._....d'...7Qp......K;..^h.\.W.../...S....-..J......&......Y..I!.P.w#...uT |....:.V...1.z%.Fn.6....N..L..$.2.?.e.s".ti

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-180_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 270 x 270, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	3673
Entropy (8bit):	7.8322183683928195
Encrypted:	false
SSDEEP:	96:nBWR5fosUcvpqnOtkeU4ghCboMmSaj+5UZy:MvHUUMnOtpz4Csz65UZy
MD5:	98B9F7A4F4322E7B46DE392FD20F66E5
SHA1:	D009D227522206C40CF592E460C9642CD03B8769
SHA-256:	A706B332E6A846357A86C30D0E8BB7697E7DD55C2AE592DD45611DDCE0C0BF14
SHA-512:	3B3E5BAF3CFC57119E0812DE2816DF6C7DCB42E96C4891E47C4F32320FD3BE2F27A0118051A6651595BAAAA30069BB1C0D78AA701744A44534CABE7547D4BE CD
Malicious:	false
Reputation:	unknown

Preview:	.PNG........IHDR.............1.... IDATx...k.u......:.....*.o..I..J...L.H.(a...1....6S.....b.6..2M...fD.M..TN.5..o qx....;g..}^........."""q2.3Qr..z.. <r....D.w.2.".r.*...s.......\..)d+.XJ.A........8Vq....g...vo.%..B..._M{.a&.XZ;.|r.v%."NaN.Q..R6....c.cN..~H..M1.X..a'%.d,=iZwF2...;.l.xU.H[..i.6;q.....#.y...w...... m.$~..$...L\E...l. .I M2s5.==.%..-....|.:,.`..........<.c-.".\....l...3...j4...B.sn@....Oxb.%.....B......$...-...WC).j..ru.s+.{.2"..5.c.q.e-...;.`-O1...@.G.F3.El.'..>$...(....d....6....%.CG\.e.[8.5.!.#....`q.3.W] X.%...$y...&...DZI....K..W.x.....%.......H+.O%../..n...~....C4...9nAZ..`..F...2.S.khhtz.E.(.CX....Uf....^&J:..@....$M......(.2..U.].O'vc...mzxlm....obq.M6....,.."H...}J'\yll..,....Jx..$/..X. uH.&.].....r,P-...[9.Q...Lr:....(..>..\|..;.h4V.%y.\|.]...$#....[[..d...U. ..B.H9..d.26.#.w..5.b....q....oq..0Z.y.NP..1.c.V!!.D=.k1.:.?.q'-..w.]..B,P..B...|....+X....j,..2q....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-80.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 120 x 120, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1723
Entropy (8bit):	7.769427546963699
Encrypted:	false
SSDEEP:	48:MtXb2ikqrN+EMaUeTPMSEGS6CT/GF2MdJtDHBkZH39Hmgwiw:CXbzrzfUsUGS6A/ETJtHBYNG1iw
MD5:	1F2FB1BF463B2FF2BEC96784DEBFEF84
SHA1:	AE6F721AD937FE39F86602F71002435B18BF1EDD
SHA-256:	7E6B0D9EA7FDA1B5CA7A0B01290521DFF943DA4CBF1498412CA7D749DB42C32D
SHA-512:	0C92C4F75E620D0B636CFD83E89C69A44F6A96A00006FBD0B13637BA5DCC77C9B302029E62F4B80766811F31810F9C20AC1A98B65C38789951CA0E19A5BB689
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR...x...x.....9d6.....IDATx......... ....s....P...m.m.m.m.m.6N......w.......-...g2/...)z.....K....~(^..`...j...z.^Sc.n.,.....0.VW..al6...a.....R0...k.Q..N..P.x.J[ol2..)o.. .A....x.....c.m;F...t.16.....L8....vb=AQ0.<.X).@....M......g.....k..,.AN...-..R......$....b..`...... %H....`6.g#..h.]q..5._.@dA..c0.;X....a.. .2...~..;.1..:.x.....q[@R....,4.w.v.._..s;.b..s. Qu5..U.\|.6Zj...P..........\...qa. ..D..W.L...c.~.....A...F1g@x....V..`..,..D.=..d.i..Q...o.c...N......$.`....]...P}.G....BT. .?.......L.n..+nG./..cC.>0.N1.\.C..B..4.l./L.3....T.c.S..bf.0..t. ..J..!.aU..p`.....0./..}.iL.).w..hc.M..'.. ..;'.p.Rt....R.g......8.%14...S....<.Jf./@..U.h'.G.R..D.\..z.4......<....*2K.S.bj.1....=.../pd.........cfPL$7....S[.M.%H.M..W..T...ZP.aA~....D...+. .~EYK.#..zOZ.]fA~...fz..].....7.>..|.........[...v..M..vb.........L....z.`.P...X..RP{.....`...+.0...l/..>...i.w...W. .....x....T..............t..+B}d*`/..+.;L...J..._...iC..pv..gA~..k.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-80_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 120 x 120, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	1425
Entropy (8bit):	7.721284228612739
Encrypted:	false
SSDEEP:	24:sRv0SxfL9UEp3g4/RjUG894TBRVPvhjfghucgXy2nRlWzIXQuohMU9ocyMDh:sRv0sq4/tU10XVPZjhy0Izy9srWcyUh
MD5:	17471BB63ED62A6E545B6B626A763511
SHA1:	586B9EFDE7B3A04580A49F8FE7739593D42D303E
SHA-256:	DFD1054F989CDEE25F19EA792F363F042A125CAB537A424F0224BBEE13607E39
SHA-512:	F619D963B62EDB07C8077C3C6AE60ED8D3F3DD5BB1D05A2B83DCA1A7A4A346598B055F6C7EA22E05BF281B1DE0F205F5D1054819000759D9450EE1FE8F6491 E
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR...x...x......m.Y...XIDATx...m..e....}....d...9]9\...r2..L..37...S..."s..SV..].t).*.I..dh.Em..`A ...9.`......./..u.}...........v].KUUUUUUUUUUUUUU...~.p.....M.6Y..l.]...Fv..W;..o..d.l...r..{.d..r....a....r.y...@..>.z..C.l.qh............7{E:d.w.W..ZD.2[.~_..y^4.q.!./;GK......Z."s.m..9...{^.g...g...i..[$"F..x.Pj9.b[E...,.q.^.......v. w...4.I.E\....D....9......C".Q. ._El0].=.Z`?.>gD....&Y-b...+E...(.f..~`..."^....Z...:\.h....S.v.v-KE,.8.....W.....Ag.V.....q..yD.<..6....x.d.N.....d..?.Q...[..".WZ&.,....v......Z...vG..k.4."...tv....".T.K.L.q..sQZ%.M3V..D. ..D.!.-.T.*b.n|W.u..xVl....X..._..."...n...5...W.?.1U7Z...p.>#.R.p..#QzJl.;D\..;E....Q..zl.w..wD.4 .j.u....D,.SE<..Bl.........U.Z.[D..._.4K..u.....mJ.e....&.m......-7*..X...:T.K.}..;~....."6(...O..(M..=.#.q.{..xHl..E,...v...3.`......X.[.E|S.IF......C.b.....r......9....o.\.x..WM..J..5.&.IJ......|...........q.J..!{t9L.Y.}D./5.."Vv|./4V.v....i...8Ji......ae18...>.q....0...X.,

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-100.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 70 x 70, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1564
Entropy (8bit):	7.78686155071436
Encrypted:	false
SSDEEP:	24:kO3Sxd5HLMZAoBjXkaBPxrX6hzB6eCvTYJSM2nY2YptQ/ceAV5ulBbYZwix2:MLLMWcV2z8nryWY2SDV5uPsqiw
MD5:	C3722E0232EC20AC8F99CCE7A040B294
SHA1:	91CA47DA87EC045ED3EF5D97243167F08FB9E10B
SHA-256:	A333D7E4293F5269426B3FCB673A284F3708A66F957DE62403B6570B24BAE8F5
SHA-512:	71940B8431E36307BA5176939A169B9259BB6B43C32529A10A12C5EA31447BDDCCAD7EB9EF7CB309B175EE7BD56E70926BD5AA0855D0FD9497547ECD7FF931 8
Malicious:	false
Reputation:	unknown

Preview:	.PNG.....IHDR...F...F.....q.....IDATx.....L../..m.m.m.m.m{.._...+...d...[.|..y.'.{8..N8..N8....x0..$.iA&..d..@r.....&X...../.z..../.....{..../u~....|._4$5..4...6....q..P..D.U...u...W ....o@#..j .o....j...r..MI.n..X.RI.]..W*g.g..;...|.D...2..._.#..$.....A.....I..r..GOF#F...L)..P.8.....G.. .I.m..J.=(+.{..@#....CH..|.:..n.%..0..*.{...O.+.Q.ORp...7L)dxS2H..Ge....e....$..k.. ..iJT.~...eZP..A2....g..PUB..|....v.......>..k..~h3...40.x...(.....v.%.F.....vl..h`>...P...4...W4.D...\o.9...z....3].....`.}t.....XI.[z..%....S<.e... .D..TA...'.....h....l...,...$7.....0,%.. ..l[Au"...d&?.j.....,..|...~F..pB...]......L.]d.v5...U%..h:}%..._$...X.m.....S.yL...Bc.R;K..8...*..TiP.}5.g..p..m..s].ZU....H.{P.!,..?.....t.U....=m-<.a.v..l$...u.T5..LG..b]...c6.19d;k%.. .3....,..l.[.1..:...YN...h.*5...W..._....dL6.v.Rch..~...i.1G....|].AU.k...H.[Q.a,6.5-....Gt.9U.....n(.#...D.v....._.*...@l.}...i.u.@..w.T%..*.&Y.:o.X..3.Z.m..fW..5.....D...

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-100_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 70 x 70, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	1341
Entropy (8bit):	7.829707677562043
Encrypted:	false
SSDEEP:	24:vHNfCYvjHq3yow73tnF7H1r8lR07iBa/ptAFjLmocqM3LNpi+MaG9vz:vHsY7Hq3QzT7H1r8Wr0/zAxfyLNp1Pab
MD5:	504D80D276ADCC0163A8E4720013F9E7
SHA1:	6D34A0593FFCE916CD19B66D61004FD7E7EB2CD1
SHA-256:	EBBE0B4761EA8968A0A3FAFB383AC7AE175E98CD31A0F41BDF5FCB43469B58EC
SHA-512:	9961259704FF97C0E1899A33259F62155B73264E272064F3FA90E64124513C7C8BD6AB69A39C1EFB271ECC2972AB8FD86FB836F22153A9BB35419C3816D11337
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...F...F.....'*.....IDATx...{L.U.....#A../.9S.&:/..%]ti...TL][Hm.n..8,gsZ..Zk....:u....IF...".I..[.H(.q...{.sx.</.....y....9.9.<."""""l%.J..2.L...xFp?...?.8....:N.M..`2.i. .M.uZZ+'..C.....9.f.1.X.}He....b...$..V..".."..T.....[.s..}..F.....t.InK..d.5...Yr..ld..x.\...iP... ....X.....a ...i.C.D.E.H.&.....Y....h..G.....1..h..C..>t...$...m..+..../.<.n4.."..(w..%,.R-. ..t.$.?..#.QB.+.ep..-.....r3.LYo....A...1CVK..$=.ER....}.o.m<.....#....D]O 1\..}..^.....,|[..L..j..`...n.,....C.N.K..U...k..(.IF.....1.....B6..X..U.....oK..cvm...tP.....lM....iAq.+...~.t.. M.&...0.....i(.y.Gq.....Zw.,.H.|... .H...zXR...>....K...)S...E.....V..H0UR*...P.....\.I.....n.fj*.*|..1...U(=.....~@=.X....Hq...4.....D..4S-...x.t;....X0.....`....j....+..X8....z.t..DV.6c.\....= Ri2.y.{ac..../Gv./....X.n..o....x..ha.d.....p..V.QRg....8...?.[Qrxo!...r....Ni.4tOHz...Ca...z.K....er....3...;...(.0..[r)6.J.3.S'..(.v....l..~t..".&Fwx..M....P....>.7.E.Z.Y.%.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-140.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 98 x 98, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2005
Entropy (8bit):	7.837796638299837
Encrypted:	false
SSDEEP:	48:FtyHJuovwDhIXRvUCvqfPAuwdESKbtU04aQkClnRU8lbPxbsFIV4hEIA:FtygGwDhIX1oHO4KwCAQ9MEIA
MD5:	667BFBAAEB2D2B372B6E0D4BF4992CE4
SHA1:	4C6C2E07183963F59391945FBEE077B55F8F6B2A
SHA-256:	207519F1C7B6C7509BFEB7B55724997EEC6456C8BAF55E882E72FC5CD43DA221
SHA-512:	AC63A3DD2F6088E7849E3824C35FD58CA78EC77DC31E1F6CBD47DE7CC394318CBA7D2309912206A94180267BE057C2AF5C835424019E2A03EE33A2AB801BA94
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...b...b.....IDATx.....S.d.....=...F...m...5.r.....m....g{.....[1..q./.D.B."......)h.a.o..x.p..r....]..\....b fR.....W.a.."..Ix.....58.G.G%D.....0lE..E1D. <...u<o...6>....-.`..FX....I\.....K.....{..Y.....D.....B.<G.....7.5...8...\....?.!j.b..F..PH..X....8."..,..R....X...((..G.0..&~a...{..DA<v.....H.4Q.u..a..#<Bk...E ..b\@'...3...U.\..4M.. .o.m.m.m.m.m..$..R9.....&..NMW..{..4].....m....h..y/..x....a.[e..7.ua.^.IC8....l0....1...r.&.....G.....c.....d....F]...M.a&.M..V..?[..t.P.Xx...*<.(...s...'.Q....'.~{_.....8....R.%..7|O.Bl..... Sr....^..@.....us.".M..?x....*.T.....A....&.I.....H`g..."...I}E.7..].=...C.gz.....V!.EE.....7WvB.!.d..vJ...k.{?.....1.n/.Q.{.....LD..;k...\....]G..S.+....F3.}z.=F(.....$..D.[.y.... /Q..eU ...]M.[r.....}.f.s..;..!...s..C...x...Y3...<....0.O.p.\..&5...f.u.....4..A..".. .ID..7.#..P.../.i. .....+...M...}/..U\...}..Ah3"t.....D...Iv..V$

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-140_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 98 x 98, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	1697
Entropy (8bit):	7.76630495035972
Encrypted:	false
SSDEEP:	48:TyhJvOYkuSoLYIWawZM7SkzaacHxXgr4RzhQpKP7C:6JWiEIOuWkCxCSzhQpCC
MD5:	93223E8777B581E988B703DF82593B17
SHA1:	40A035464C27041CCC87C7935C45100D93D1C948
SHA-256:	464AFAF960C32ABDC2C3937A48BF14C5D1A819B017E719FDED591D43A65D94C4
SHA-512:	B8A3EE4A71E609625EAB51F0F6DAFCC82CC47BA2C567CC8BF73CF6423056F9171276289BFDCC8428B7C07645097664065EE9B0B78874425BFF800178222FED1
Malicious:	false
Reputation:	unknown

Preview:	.PNG.....IHDR...b...b.....hIDATx.....9.Q.f..ttS....u....%..1.a.s.!f..c.b.b.K7QFg3..Y..2M5..6:B..z9.%..N.s>9.{.=.....|.7----------..QNt.G..].E.....b.s.e..X.C...Q.b.;.p..m.....g....L.\te.G\.d...F..X..=f..]y.A..\e.t....Ei"...d.X...X..7[TYh.1J..g...y....]/.,r.....mi..2.6J.6Yte.....g.....<o...;..v.T..KJm..\T....i...G.."Qe.c..1.I.T#.6...2...7.y.K.*".....p..J.2S.V...zf..Z%b..Z.6.z._j.}K..w..R.2.Y..M...P..I..d.JG..Sm..0V..o.u.'R..6...(U.k...k.+m..i].n.ub..D.b.JwJ.....-1..(. U..|.^....(."UO..z;.@,2Vi..D,...;K.NAi.."f.TO.j.XlO..}$..M6..".iC.."..MO]-..[()"U.i..E...J.K..zn..".V..M..i....q.(=%.5...R.e...:P."..(.*U..[...M.G~C.....Q3)..]o.%U.*./.c....t..:J...q..k...g...R....\...A.@.kl...H.vJ...x..../....9.:..?q...Y..":@i...4f..E.Yi.T]^.....Q..#..h.#"...4S.y.I...AiG.kl.QWI.nJ.E.F.}M.tP...9...U.f..g...../....]..U:N.{..B..A.2..i.Ru..A"..+jg.kE./Ru..R.g.D...n.q..X-b...f...b.+.q.....gD.Y.....q.....t..kA.."&j..Ru..."...j..D..4n.S.wD..gG.x..

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-180.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 126 x 126, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2699
Entropy (8bit):	7.8799233652993115
Encrypted:	false
SSDEEP:	48:ls+9LgA+9fj19UhKwdgrviOztr/CrWbqCLRTFxFCEEgq0Ol81sqAGz:llSN1gBTOztr/jbzdh1y0wl1+
MD5:	704D0A2693B350E7C463B0FF2143835B
SHA1:	0313AD4C3690A590AC54552D2C27806E73776600
SHA-256:	D6367DBC074E37F3488C26B0BAD229BFE99F5C6BB0E28D37B41906C436152B57
SHA-512:	4517B2FA911149885EC5549F3173D3C774716740826873E4B2199C804B17E776A5296565930E5ACDB8D5476710A391B21E6DA8941DF64C525A487DB4619A1EA7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...~...~.....#.....RIDATx.....f..`....6..m..j#fm.qm.Am.m.....%_...q.i-.>dh.....q.o!!..]...LC.TF..D.o.8...8.O..|.iLC#$PO<..1P.....wX....J..<5...$`O1.YU..g.L....<.....h....K.4Aw.....[.I...yU)....D|..x.....`f.....9f....Y...p..!..E..U%...]....I.#.....#gPB.5...^C4.G.....g...5R... .....W.~H@. .*....8.....G...N.U...c....J".....YQ.m0...b.5.V.Y...:.....(W1.E...yb.,..a.bT.^.O!a...6...+!:.*..|O1.....ZQ9...M.6.....!.6..O.XI...#jF..w.o.#|c...%Y.h.m.m.m.m.m.....8.qog.N.....3.}...R.....8...P.M.....]....B.....3xs...:M!...K.;.mL.7I.N..=..7.....sfJ.;..|Q.....}:m..08...y.+.5...D..:....|8.m.]....04Z..b.....c.r....|.....m.6/..!...Y..)4._..0KY.e.[.qL.!...X ..jk.....|.....Ki....q...28...-.....<....4.d`.Z{.-]|B..3 PJ.gP.iW-..]m..61c...8.b.,.. P?&.0.....A..!_k`.\.s.>.....d..R....'"*<.e../.A.S .+...O.Oq.&.B.Y.6...S.!W^..... ..3.A..*...GA.uX.|[..Oh..=..[..9....I-.I..+...mM..Xu_.#)..

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-180_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 126 x 126, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	2334
Entropy (8bit):	7.8839656878677005
Encrypted:	false
SSDEEP:	48:W/zeI9zj1u/VwgVNR+vEgxOfU99BpcZlp9uqRhq4eZDU0BMK:W/zn51gxN4RxH9hUlpkAMt/BT
MD5:	39E2FCF13C20103C5F449C06D3A4CF75
SHA1:	AE8E1BCE2BE17ED450D891864E6AA22642AF39AC
SHA-256:	5D46E4056F3915C279F1FA9EDF61D93529FBCAE5C59D616380EC5D9405B7763D
SHA-512:	8E4902262B064008804D49D1B5F27BB7B8F33ECEFB05181AA69534E1D21662719DD4F8E0677C58215F6C5CA9EB4FB92FCA54A89F9720230AFBF06A70216ABF26
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...~...~.....H*m.....IDATx...{p.....1\0<.%.1<.....L.(.0P....R.(Hkk.3.>(-.X.t...>.Q.....#P.H.JECxZ.<...5...${.7...../...g.....x<.....x<u.0.Y<.f.s.r..7..1.Q.#.#...X...C\|.r.....h...b.e..D.[.H..RG.q..f\.9RhV.y....<.Z..0..K.9.c.s(.C9...d=.4..YJ.V....l2..Y,.....u..kH&.....rFh.Na.k8A%J..<.-D...Wc.EL'..T~.....I.....N..F...<E.Q$.*.-N2..a.D..;H Jt..%q.....ml.....3L$.n..-.Ha0SX..\.#..w..28..W...Z.....Y.....o.....v5.....|...xv.X.G5m.e....tzq.e.7.G.r..Q...D2l.^....E)J..14.....~..HCg8...JZ..TN....id..I...3.Vz9...` ....%3.F..v.JG'....Y....,Ic"-K.]y...h.m.0C.I....".(Gq....g.S>E#....C..+.....].u...+..I...g....b.H....3d.S =.O,.7[...q.|.6/..U.U(.ed.,....DX{.JA}.im;..)..Id.p.*?....QK.....H..i.....#.~&=.&....pZ..&.2....J.s....p..r...y.e.....c..3.g.H.z".#....C'M.h...?.....v...&"...z.e(i.+Wz].....<....?....M+s.&....d....*.0n.....s...<Ws?I....?.{...`5z3..w8.....s.B.d..K..K....LLY.j..^...a.p.~.z....-.....I.dM.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-80.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 56 x 56, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1096
Entropy (8bit):	7.755097954664401
Encrypted:	false
SSDEEP:	24:TDh4JYYFMId219dZt07Zcglb4iS/cFEAAabL3/006Fs:B4JBMPVEbCe/006Fs
MD5:	32D3E390613CDDBD639E70DDB2511AC0
SHA1:	C96AC088E72D756F31896B16776EF100379F802C
SHA-256:	DC20E5AA2B500CD5B5C9F89647D3487810685C94268F22678E27820E2454BB3E
SHA-512:	7381CEB8FEE84F398082177F30DC01593BEEFA729C73B0166AF686BCD25D54312B202D9243834B754769DE41E9A1DEED74CA91A76DCDA918A749CDB4F08C12B
Malicious:	false
Reputation:	unknown

Preview:	.PNG.....IHDR...8...8.....;.....IDATx...S.,I....[k.m.m.m...k.f....0..Ag5..<.w.1...r:..g.+...+.....MX.k`=I.....\(.....,vDq>.....x..`wl.U...x..[.....(..p...@u..z...1M../.D>...z..'vJ..U. .'C.....?c:..U.....GQ...,.P.T<...-..\$~....q..n=L..iF....X....q.....p.6{q8.u'*.R..C...Qg..YCN.:.....#g^.R...w.....U..j...H5..eF.....iO`..4r.R.[.....0...9{....u.v....X6!>.F`*.Nk.....J...5. P..}..F.\..Lk._.`.#...od..7..4!V.....-...{r.P....9^5.2.(.G..OT..<9}1....A..Q...U.{C.....o..S.....S...b....z..T...o....z..Z.xv.....O|.8.....u.....c...?.....u.u.....p4.v`.....kQ..4.....jzf.^.... F..4...j:..._K.;..z]..0.0>.....|..W..Z5!6.b?....2O.....,.>.Q.y..-...._...k..w.}.V....s.o....W*..._Q...X..=Tcmc{N.P..1..j..'...l.-.?j^2..*~}Zo.J..7..F....D.91.....#2^..7.}7.....$.:P..oc"6l..)n... |A..G.....l'..x..bM#.|...e.yT...k..y.]9...2.ao.z~.g`4....e0L.....t....n*.....}D.>.O..Vv..vE.Qs.\.~...s.....v.....T..7..A.9.s.]zQ...Gb.q).2....e...

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-80_contrast-white.png

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PNG image data, 56 x 56, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	901
Entropy (8bit):	7.682141855410327
Encrypted:	false
SSDEEP:	24:x2BZqWXRHKkqILfEDtySHnb98XPA8KWstHNMufZ4jJO2C:xZQEC8BywBmPAGpC4jJa
MD5:	E6ADD5AFC73F7B06FC2348550595F8D6
SHA1:	4D658BDDB93FA6CB423EBC61BD20DB37E4D37DB6
SHA-256:	DD6F46D32C3E235508F9E4C7D7F993BD807D955BCA7E63CF3D57C6C4C102F46D
SHA-512:	55437DFEA7F68A4572DFC86B5428CBE9DB86C0D32D0B09BA6B7B1CF8E49E5F1BB94285BBDC97D8EE00D70BA75921DB59644787C1BE1672FE37CEE09441F249 B6
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...8...8.....IDATx...mh.e...c....#..."aM..f!Dh....eFaa.....0$3.a.bS.(!..$..@%1-+.,.ge..\.9..=<...}...=..7.\'7.-////...T.2.x.F...Ur.5.v..L....Iv..-..a.1&...Y!...U.S%..a. .....k.V!=....'..M.Pl.F!..s.V..B8g.n..9a.....Z.k.....vH..i]V.Yx.....ve:R.I-.c.d...\.....S.s<.?....`....).Ab.za^.s.1....~r4[...6a.....$6.o.I.z..A.Z.HG.:.r.C..E..<+.#Q..P.J._..xYX-...[l.'l.o. {...Q.Y.E.'.V..3...H.....i'.w.....:a<...W2.I..0P8(K...IL.V....).V.....=". .....;.,...F&..U$6.....d...e.T.}aK...4I.!.(.U."...,}-\G.Rx[&..O...$Kk.I$.k.[&..c.....S,.v.....(.Ao...,...K[&T.. \|.....G.G.6a.++t\..*.?...La.....F.....r9..t.U.9.DG.8.o#..j.d..L.~..;B....e.f....*,.....b{./.....N.....`.e$npL.U..f.j.I..A....Oa.^.F.N8`...xU.....@?..t%$.,...I.n)._h0/U.d.....I.C...I....R..) .....3H...N....h.9j.2.{.n_...y..m.9.5.^...H7.i.A.....e.?..R....]....IEND.B`.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\CUESDK.x64_2017.dll

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	485344
Entropy (8bit):	5.205905061365067
Encrypted:	false
SSDEEP:	6144:alTZkQQzVVTgmAffw5QTzL6+75I+qZojZdJ:azkQQzVVTgmAffMQTjO+xt
MD5:	943CFEC00D31592C1B09C1086CE5B39E
SHA1:	DE211386FC16BD90C5D0D9B2527495D36424A131
SHA-256:	D2C6E0E2E2C24A1AE11A8D638A5EB11D97F0279946874D13E893AFA520DBD2FE
SHA-512:	3728349851899E36EA6B1EAD07BBCCB651661D8B76BDBB199C6B42EF9D56DB4DE9A1F7BCE55DE2AA32A9ECAD44BCC00785519F1FC5BFCF5B6A1F50551B98 CE9D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.y...*...*...*.xE*...*.h.+...*.h.+...*.h.+...*.h.+...*.f.+...*...*p..*ci.+...*ci .+...*ci)*...*..A*...*ci.+...*Rich...*.....PE..d....v|_....." .....N.....L.....5....`.....#.....`..6.....,F..."...E...p..(...@...8..... .....`...(.....text...hM.....N..... ..`.rdata...)...`...*...R.....@..@.data....*.....|.....@....pdata..TN.....P.....@..@ .idata..X!....."....@..@.tls.....@.....@....00cfg.....P.....@..@.rsrc...6....`.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\MEIPreload\manifest.json

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	4.824253848576346
Encrypted:	false
SSDEEP:	6:v5975JVSS18iMkh26VlcmutLwyAGI/zj//gQNMC:Bbt18l+LIMLqGU/gQNMC
MD5:	442699C95B20A60470421C6A4D29960F
SHA1:	C7317F2D2414C991C21205BA3C68A187B997E3C1
SHA-256:	44844CF3DDE6E80087AE0E6BF0D9326D7EF7D23326D24AC83AF0850BE26923D2
SHA-512:	C89CF089F7FEEB80C6DED11F1FCE84287ABE8216A6E05723D1A7FAF567C501C043CD1246FF8DBEE1240D2D79C41B698EF4CC3459589E68E5BFC5BED7FC3A1 50B
Malicious:	false

Reputation:	unknown
Preview:	{. "name": "MEI Preload", . "icons": {}, . "version": "1.0.7.1652906823", . "manifest_version": 2, . "update_url": "https://clients2.google.com/service/update2/crx", . "description": "Contains preloaded data for Media Engagement".}.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\MEIPreload\preloaded_data.pb

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	8254
Entropy (8bit):	6.795641289553097
Encrypted:	false
SSDEEP:	192:bTOpyeS7AOv6EVp/m3FPKk15jjKVcOmQppXavFbeLfzrLyp:bTOk7AdEugo5jjK+5QppXaBebzrLyp
MD5:	D5E4C2634EFF8A9B3FAF432BF406D6D1
SHA1:	A691F5C9877079193C1F7DFB16DBC30BB0372EC9
SHA-256:	C6070A157B4E28D16FBCCBD233E93846DDB070C85E1A1BC64469B7A5F1424FAD
SHA-512:	B264E28AC8F111DF01C553445AADC7BCDB3F32A38A1A19D3F9D458270DFEAF80EFA7144407BD999892022AF9DDE9DBF8A0E19E7212720E1C6511EA9125AFB166
Malicious:	false
Reputation:	unknown
Preview:	..@5..0@...@y@o@.AK@X@.@w.!@.@.@.A.A.@.@B@.@.@.<A.A2A_..6strea.....kpo..anim..^...elo.tele..g....pan..bancidiz...don...lkor.....D...ap.cuem...ukleren.squl...ve..vco.. ....sten.tid..+v.....dou...myvrs..=bb.jl..#streamfai..P2...nkk.....10...f..R527.....p...7.....85.231.223....11.90.159.13...movie..w23serie...3tv.co...h...pla...00mg...bstrea..W93.178.172.11...49.56.24.2.....secure...|qo.....routk..nitetv.roge..}map...ndavide..ci.t...view.abc.ne..O...j....lianonlinenetw.....r..'oora4liv.....8.topgir..33.sogirl..rshow12...ayospor.....mc..s...k.....sian..nime.c..n.....prof..ba..Mtochk..Zkra..Tg...-....K.....@.'..2.vos.....m..rig...r.. .....@g..>.....perpl..)...tualpi...gintvgo.virginme...eo...mbox.skyen..@aplay.O.E0B...d....W.....portal.jo.._...e...ma.....Lsearch.ya...frida.....a..Qhnex..jvarzes..ey.....e....y...d.tv...stfr.....l.....seigr..U...d...q.....z....serial...r...cuevana..Amovistarplu..a.....f

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Resources.pri

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	3.118957212117411
Encrypted:	false
SSDEEP:	48:Whs+6rek/gF1A6Gbi+4eTy8iPTUucUITUuqQTUGUQTUsITU6UQTUQITUuUQTU0I0:WWnep/FFLxPoRJo+oGpoBo6po1oupop0
MD5:	400817D0A91767CB830767AA94383F31
SHA1:	73F36C895190223F94E4D52657F14454B2BCBA44
SHA-256:	35D92C86C1C054D1C03F4E58B83681BBFD8573143EE5E4CFB4CBD788A1FFC107
SHA-512:	2216DFC65E24961A18A4622FF6D8D8A1330283E64477A0E44BAC5B8F9A4CB5690FC90F598BBC152214EE6AA8770FE6608C4C809EC6F2CC73547D8166603B3E1
Malicious:	false
Reputation:	unknown
Preview:	mrm_pri0..... .....[mrm_decn_info].....8...[mrm_pridescex].....8...H...[mrm_hschema] .....[mrm_res_map__].....@...[mrm_decn_info].....8..... .....W.H.I.T.E...8.0...1.8.0. ..1.4.0...1.0.0.....8...[mrm_pridescex].....H.....H...[mrm_hschema] .....U^.....m.s.-.a.p.p.x.:.//.O.p.e.r.a./...O.p.e.r.a... .....L.....F.....A.....O.....1.../.....7...!.....F.i.l.e.s...A.s.s.e.t.s...O.p.e.r.a.P.R.I.C.o.n.f.i.g...x.m.l...7.0.x.7.0.L.o.g.o...p.n.g. ..1.5.0.x.1.5.0.L.o.g.o...p.n.g.....[mrm_res_map__].....@.....,.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\assistant_package

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2973528
Entropy (8bit):	**7.995948649674358**
Encrypted:	**true**
SSDEEP:	49152:npr0nnDiGZgF23VzfajZEGXGt+TR5P/H2iYyhQivUa6Ta7q1nt89qtTme/dLnUgq:nKnDhZgqajZEqZHXWi7+Tau1ntuiVL9q
MD5:	128F7E7285E953D6EA26A318D7A7403A
SHA1:	6423142BE97D4719C8A0F775EA73569E233200DF
SHA-256:	550C9209EEA87801ECEC9B2435BA7C5BF333DF38BBFFEE4BBCF4CEF2D0F9FCBE
SHA-512:	0018FE73D26BB17877F69AEE8D480A3DD51A55C3B3E1904990889314A04D829D87E78381475EDD0BB23597DCB4323FA379A5395342EA9D117750D3E3693059CD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	unknown

Preview:	MZ`.....@.....`.....!..L.!Require Windows..$PE..L...'..P.....(...F.....-.....@....@.....@.-.....b.... .....5-..).....@..d.....text....&.....(..... ..`.rdata...5...@...6...*.....@..@.data....).....`.....@....rsrc. .....h.....@..@.....U..`.A.....S3.;.VWt.f9.b.A.t...`.A.P....P.|..Y.nj'.v....u..v..=.BA..6P.....P....9^..].v8.^..3.....hhDA.P.....P.....P..pAA..E..E....;F.r.....P.J\|..Y .24..j...IAA...t$..D....3.9.H.A.t...@....9D$.t..t$.Ph.....5@.A....BA.3.....D$..`...\|$..u..@.....3.....t$..D$..t$...`.A.....t$...P.Q..%`.A...D$...V...t...P.Q...^...VW.\|$.....t...W.P.....t... P.Q..>..._^....T$..L$....f..AABBf..u..L$.3.f9.t.@f.<A.u..S.\$.V..C;^.tLW3.j.Z.....Q.....3.9F.Y~.9F.~...f..Af..G@;F.|..6....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\d3dcompiler_47.dll

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4927400
Entropy (8bit):	6.402970220950094
Encrypted:	false
SSDEEP:	49152:VCZnRO4XyM53Rkq4ypQqdoRpmruVNYvkaRwvhiD0N+YEzl4og/RfzHLeHTRhFRNh:0G2QCwmHPnog/pzHAo/A6
MD5:	DD88837D51ECE6061718CAE0A638BB60
SHA1:	02987B303D9F27C7FC8A093C0CCA32112E9ED1B0
SHA-256:	AB6FD3AB40931DFD337C5D4D34B95F44A0BDD44D56507D740D97278AB254139F
SHA-512:	B2C7F4FEB2D323DEC2455710F6B04EF9642803FEF02936DBE5A09FC00453F8CBE2CE2E93BA2E5CDE537DAF7342BB14D6C0D49D1700AE86C8C2310863E3FB33 8E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|3..]...]...]..e\...]...\.5.]..e...]..wX...]..wY...]..e^...]..eX.y.]..eY...]..e]. ..]..eU./.]..e....]..e_...].Rich..]..... PE..d...^.}`..... " .....8.....<).....K.....L...`A.....`%G.x....(G.P.....J.@.....H.....J..O.... J.....p.D.p.....S<.(...pR<.@.....S<.(.....text.....8.....8..... ..`.rdata...F....8..P....8.....@..@.data...`....@G.....@G.....@....pda ta.....H.....@H.....@..@.rsrc...@.....J.....@J.....@..@.reloc.....J.....PJ.....@..B.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxcompiler.dll

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	21868960
Entropy (8bit):	6.5327904051612276
Encrypted:	false
SSDEEP:	393216:lkwXSvzEhmbfrZV+m2iG890hvCUD/GVJkshSB:KvN/GVJksAB
MD5:	B4B0BB9DC73D5D4B45E35B5CEBB46609
SHA1:	6CD3DE6BC604180F7E3BE7F052F0D1BC67ED7605
SHA-256:	AA5D6EBC4765063FBA4D02D24D9FC4B5845D5C8F86418EF7B8514B3C05EDA306
SHA-512:	44DA8661C4C6368FC046C99916B2109EB763B7D9EDBEA66B1EB70A651C018DEED91C8EE2F3269B10591ECFC082C85D43E6ECA555BEADBD1B83C898ABC1B2 CCA5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	unknown
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d.....f....." .....F.....M.....@N..... M...`A..... .p...H. .x.....M.....B.....M..)... M....DD .8..... B .(.....@.....p. .....text..... ..`.rdata...~;.....;..... .....@..@.data.....@B..n...0B.....@....pdata.....B.....B.....@..@.00cfg..8.....L.....4L.....@..@.gxfg....0....L..2...6L.....@..@.retplne.....L.....hL.... .....tls.....L.....jL.....@...__RDATA..\.....M.....lL.....@..@.rsrc.....M.....nL.....@..@.reloc..... M.....rL.....@..B.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxil.dll

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1519000
Entropy (8bit):	6.516243319485896
Encrypted:	false
SSDEEP:	24576:LCfhbh3v3mtZDiAQeWj26k41ob2nrZ1rqpegQDJqoZtp22GkmgA9u808jQPEdkrT:LCfhbh3v3mtEAQrW41obCraeRhy9ou6p
MD5:	044B9B2A5E1CEA24BDEF3A3A81C9B9D6
SHA1:	E96670C0681507CC9926CB475AA28A8C9BB7D529
SHA-256:	3FAA3A0B1DD6AD2BA2855D6F82376E223B18A51A39159F5923F2AA33668211E4
SHA-512:	A1A41B79884A615D226F744960F666BD2991835A796117278C7D8426217F384A127DC6040C04B1F4BB2707B5BB4464C562CED3881A8FDED6C02263C23B358C1F

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@AC.. -.. -.. -.OX).1 -.OX... -.OX(.. -.VU(.. -..R,.. -.. ,.. -.OX$.. -.OX-.. -.OX.. -.. ... -.OX/.. -.Rich. -.....PE..d...'..}....." ....."....@.....`A.....I...I...P.....`.t.....O... .....o..p.....o..(....m..@.....text...\..... ..`.rdata..F.....@..@.data....{.....T.....@....pdata..t....`....."..... .....@..@_RDATA.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	405802661
Entropy (8bit):	7.083358086913577
Encrypted:	false
SSDEEP:	
MD5:	5A0409605B7CD1C21C44D2AC71C71610
SHA1:	D08FC7214FE9BCF860DC8ABEA9C7A0049263BFF4
SHA-256:	2BE333D303ED3E5FDE88637A5DFA0AF56E5047A7413B7E6B3D372A7DE7C8BEB5
SHA-512:	4D2BF9BB50C98F39CE5B4E116D2F73E33090037CC529121D445F66E90527C71D6FBE2C11EBDE36CF5F4AD49EB4500E2751AA273800F93F549458EECA30E3431F
Malicious:	false
Reputation:	unknown
Preview:	<assembly.. xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>.. <assemblyIdentity.. name='107.0.5045.79'.. version='107.0.5045.79'.. type='win32'/>.. <file name='opera_elf.dll'/>..</assembly>...PNG.....IHDR.....<.q....LIDATx...1..... ..6.^`.....{.....m.m].m.m.m.....[s....._.....N.Nw..._w..P...R.....`.....[.i1...`.$.....C.....*.,,..v.l.>.ZP.B...E@.....!?d..!.d.R.....g)0...^H[.u.4.k`....0<.d.1.....0...Q`..I.._T..!...|pG.m=..a&.e.U(...C...n.^`.....FB.X...Oio...z!...:.Tx.8;..9.[a.....{.~.^.....P.].r..d..A...?....<y.v".....l.....^..._.....MA.o....?.>u._.d..`.....E.@.5.....E.....R...A..O){.k..2....jx\..5U.a.%."#.nA....6.!..W2.....R..j6r..v...."....N.GA..8.....>..p..#..,X.....Q...y..#.a..)....Q.e.zc\.'@.AI....io....=.....D.....F.....A#6.^.^.Ma5...b.b...D...+.P.. .[.o..z....,...#<U.0.O.#..Z.....Q{...jA..ka|}...q.s.y^.!.Gh..R....t.g....F.....g

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	
Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4186
Entropy (8bit):	5.234993793603558
Encrypted:	false
SSDEEP:	96:t0/Rtp7yTf85XZylTJhowbO7VtiORFnbwU:Gaf85XMbwbOHiORFnbwU
MD5:	2DC8E2607CA1F7C321FB559287B7CA22
SHA1:	C1C7BF3A567FD2D24C348C3C954FEC3E00F96AEE
SHA-256:	269738732DC4756D0955EF9BBA7DE3A4DD025C0A868EE84E3FFC486817F63672
SHA-512:	080FD30D024EC21B7E50BBDB2FFD69E7E700B2D923171BFC2E47C77E510D663F5DAAFD702017A61C6D399E17705678E182D5F0BF53505181D864F533EEA22FD1
Malicious:	false
Reputation:	unknown
Preview:	107.0.5045.79.manifest..CUESDK.x64_2017.dll..MEIPreload\manifest.json..MEIPreload\preloaded_data.pb..d3dcompiler_47.dll..dxcompiler.dll..dxil.dll..fonts\Inter-Black.ttf..fonts\Inter-BlackItalic.ttf..fonts\Inter-Bold.ttf..fonts\Inter-BoldItalic.ttf..fonts\Inter-ExtraBold.ttf..fonts\Inter-ExtraBoldItalic.ttf..fonts\Inter-ExtraLight.ttf..fonts\Inter-ExtraLightItalic.ttf..fonts\Inter-Italic.ttf..fonts\Inter-Light.ttf..fonts\Inter-LightItalic.ttf..fonts\Inter-Medium.ttf..fonts\Inter-MediumItalic.ttf..fonts\Inter-Regular.ttf..fonts\Inter-SemiBold.ttf..fonts\Inter-SemiBoldItalic.ttf..fonts\Inter-Thin.ttf..fonts\Inter-ThinItalic.ttf..headless_command_resources.pak..headless_lib_data.pak..headless_lib_strings.pak..icudtl.dat..installer.exe..libEGL.dll..libGLESv2.dll..localization\bg.pak..localization\bn.pak..localization\ca.pak..localization\cs.pak..localization\da.pak..localization\de.pak..localization\el.pak..localization\en-GB.pak..localization\en-US.pak..localization\es-419.pak..localizatio

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list.1711736395.old (copy)	
Process:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4186
Entropy (8bit):	5.234993793603558
Encrypted:	false
SSDEEP:	96:t0/Rtp7yTf85XZylTJhowbO7VtiORFnbwU:Gaf85XMbwbOHiORFnbwU
MD5:	2DC8E2607CA1F7C321FB559287B7CA22
SHA1:	C1C7BF3A567FD2D24C348C3C954FEC3E00F96AEE
SHA-256:	269738732DC4756D0955EF9BBA7DE3A4DD025C0A868EE84E3FFC486817F63672

SHA-512:	080FD30D024EC21B7E50BBDB2FFD69E7E700B2D923171BFC2E47C77E510D663F5DAAFD702017A61C6D399E17705678E182D5F0BF53505181D864F533EEA22FD1
Malicious:	false
Reputation:	unknown
Preview:	107.0.5045.79.manifest..CUESDK.x64_2017.dll..MEIPreload\manifest.json..MEIPreload\preloaded_data.pb..d3dcompiler_47.dll..dxcompiler.dll..dxil.dll..fonts\Inter-Black.ttf..fonts\Inter-BlackItalic.ttf..fonts\Inter-Bold.ttf..fonts\Inter-BoldItalic.ttf..fonts\Inter-ExtraBold.ttf..fonts\Inter-ExtraBoldItalic.ttf..fonts\Inter-ExtraLight.ttf..fonts\Inter-ExtraLightItalic.ttf..fonts\Inter-Italic.ttf..fonts\Inter-Light.ttf..fonts\Inter-LightItalic.ttf..fonts\Inter-Medium.ttf..fonts\Inter-MediumItalic.ttf..fonts\Inter-Regular.ttf..fonts\Inter-SemiBold.ttf..fonts\Inter-SemiBoldItalic.ttf..fonts\Inter-Thin.ttf..fonts\Inter-ThinItalic.ttf..headless_command_resources.pak..headless_lib_data.pak..headless_lib_strings.pak..icudtl.dat..installer.exe..libEGL.dll..libGLESv2.dll..localization\bg.pak..localization\bn.pak..localization\ca.pak..localization\cs.pak..localization\da.pak..localization\de.pak..localization\el.pak..localization\en-GB.pak..localization\en-US.pak..localization\es-419.pak..localizatio

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Black.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 39 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter BlackRegular4.000;git-a52131595;RSMS;Inter-BlackIn
Category:	dropped
Size (bytes):	414140
Entropy (8bit):	6.13273327924002
Encrypted:	false
SSDEEP:	6144:s3unFMi82w/+qnJWPziKSQSzzY6XqYQ0rBfmPbPGxGl36DNoAmFFhGj3k4yhP18:s3uV82wWqsPziK4zbBOPb96DNAV8
MD5:	4154321279162CEAC54088ECA13D3E59
SHA1:	5E5D8C866C2A7ABFD14A12DF505C4C419A2A56F7
SHA-256:	6BDEBEB76083E187C7AE59420BFC24E851EDB572E1A8D97C1C37B7B2DC26148C
SHA-512:	04CA175774CBE3F2D83543C01CC388E2715AB7B1378143DB41BACDC7E7EDDF05D3BEEF476F6ACBE7DDEB34861984EFB5FD7F299EC1820697C440B372D258AEE7
Malicious:	false
Reputation:	unknown
Preview:	.....GDEF.m.v.....GPOS<.,... ..@.GSUB..B..F...]@OS/2 .....\...`cmapL.....d.cvt P.....A....&fpgmb/....B.....gasp.....A.....glyf.3.J.....U.head0%.a..^T...6hhea.....^....$hmtxE.)...^...-.loca.;w....h..-.maxp.t.....$... name.i-....D....post}.....xprepldhL..P.....I...K.....J...L.Z...].f..i.w...z.|...~.....(...*.,...../.0...2.5...8.;...=.N...P.P...R.V...X.q...s.s...u.v...x.y...{..... ...).).....0.3...5.5...:.:...<.?...A.C...K.K...M.M...Q.Q...S.T...[.[...].]...j.k...p.q.....%.%...).D...G.I...U.V...Z.b...d.u...x.z.....P.P...i.....`...c.....!...#

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-BlackItalic.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 38 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter BlackItalic4.000;git-a52131595;RSMS;Inter-BlackIta
Category:	dropped
Size (bytes):	422324
Entropy (8bit):	6.159556140030877
Encrypted:	false
SSDEEP:	6144:PtBc7UQ0dNXWqSBQVUWrqIWqH70TVMYydoAF4N0ELhwnftLu+hNHzFxo5spvD3+p:Pt2+dRWqgVrwYygLhwnfhjh9fZ78
MD5:	C5C41F7587F272A4C43A265D0286F7BB
SHA1:	916224C963D04B93ED54CE7C201108F398E7E159
SHA-256:	D549110689CDDE0821CA2C7148F7B47A097166B4169786A4A9EDE675F5CE87F3
SHA-512:	D4B4D01088D9F506368DC19D709B4BA6BE764929B0DD05775841E14CBBEC674F216B81515AE529E95ABFD22ED2F3E2D2774363DD4284C8C8B57D203599555F7
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOS2-.....?4GSUB*|.@..D<..[.OS/2 .B...,...`cmap^.....d.cvt O._..a....&fpgmb/....b.....gasp.....a|....glyf5.....|.head0;.`...4...6hhea.....I...$hmtx..4.....-$loca.....-(maxp.D..... name!.,.....postz.....}.prepldhL..p.....*...,.....;...>.H...J.X...[.]..._.`...b.y...{..... ...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.|...~..... ...".$...,.,..... 2.2...4.5...<.<...>.>...K.L...Q.R.....%...(.*...6.7...;.C...E.V...Y.[...g.h...m.n...q.s.....1.1...J.d...f.g...n.n...p.p..... .....A...D.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Bold.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 35 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInterBold4.000;git-a52131595;RSMS;Inter-BoldInter BoldVe
Category:	dropped
Size (bytes):	415072
Entropy (8bit):	6.167283324857092
Encrypted:	false
SSDEEP:	12288:k9zC2w597PziK+bSvkK3sgUN8HkC48AeIVMhQ/8:e4iK+6I/8
MD5:	8F2869A84AD71F156A17BB66611EBE22

SHA1:	0325B9B3992FA2FDC9C715730A33135696C68A39
SHA-256:	0CB1BC1335372D9E3A0CF6F5311C7CCE87AF90D2A777FDEEC18BE605A2A70BC1
SHA-512:	3D4315D591DCF7609C15B3E32BCC234659FCDBE4BE24AEF5DBA4AD248AD42FD9AB082250244F99DC801EC21575B7400AACE50A1E8834D5C33404E76A0CAAC834
Malicious:	false
Reputation:	unknown
Preview:	.....GDEF.m.v.....GPOS\.N.... ..KhGSUB..B..P...]@OS/2 .....`cmapL.....(..d.cvt L.....E0...&fpgmb/....FX....gasp.....E(....glyf(.....OXhead0|...bh...6hhea. ....b....$hmtxDt....b...-.loca.0.....|..-.maxp.t.....8... name.D.....X...Vpost}~.....xprepldhL..Td.....I...K.....J...L.Z...].f.. .i.w...z.|...~.....(...*.,.../.0...2.5...8.;...=.N...P.P...R.V...X.q...s.s...u.v...x.y...{..... ...).)..... .0.3...5.5...:.:...<.?...A.C...K.K...M.M...Q.Q...S.T...[.[...].]...j.k...p.q.....%.%...).D...G.I...U.V...Z.b...d.u...x.z.....P.P ...i.....`...c.....I...#

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-BoldItalic.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 34 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInterBold Italic4.000;git-a52131595;RSMS;Inter-BoldItali
Category:	dropped
Size (bytes):	420068
Entropy (8bit):	6.194498558176303
Encrypted:	false
SSDEEP:	12288:xg28OmWqgaGeWLF7k/oONd1P+yyZQl/xFiwRi98:SZG17k/oOX1PXyqCwRi98
MD5:	C4C47E3D7ED51A6BB67B7B8088A4B0E3
SHA1:	B190F4E4E8F838C46FFE9507D966EA4D8B37D8CE
SHA-256:	5E606F805A71432D4875DE7DAB737BF9DEA1187090F0A5190DA9B1BBAB09F57C
SHA-512:	B4251618479C52398CA71CFC61AD88230A14145771EF1085AB9288486D7BFC841F0EA222909F8BA6882DB6076DF26BFE37E1C23917569270C86D6E7ADEE7CF13
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOSU..F.....IFGSUB*|.@..NP..[.OS/2 .....@...`cmap^.....d.cvt L.....X....&fpgmb/....Y.....gasp.....X.....glyf.L.K...0..i.head0....x....6hhea.....y....$hmtx...T..y<..-$loca..OH...`..-(maxp.D..... name.....bpostz.....}.prepldhL..g.....*...,.....;...>.H...J.X...[.]..._.`...b.y... {...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.|...~..... ...".$...,..... 2.2...4.5...<.<...>.>...K.L...Q.R.....%...(.*...6.7...;.C...E.V...Y.[...g.h...m.n...q.s.....1.1...J.d...f.g...n.n...p.p..... .....A...D.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraBold.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 39 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter ExtraBoldRegular4.000;git-a52131595;RSMS;Inter-Ext
Category:	dropped
Size (bytes):	416228
Entropy (8bit):	6.155971405270021
Encrypted:	false
SSDEEP:	6144:3VpTx/VCC2wfBsJWPziKSQVE58IqsfnHGR4tGX5/2nHTAl84RSnj3k4yhT18:3Vp+C2wfBDPziK+4suO49lfR98
MD5:	5061BD7701B1B3339F0C80E69A2136E4
SHA1:	4A028F1FA4DBD6B4BFBFEEC4A5B5E222A005B563
SHA-256:	3C13487B8F2EBA0A78CAD4CEFD19272B0F4E53D61C223E6B266DDF0B332E9F1C
SHA-512:	65875F9F205CD70D2E1B86FBDA2AC8875637E0B3E0BB37ADE9DA20717B0F17D2108A0CF2AA1B246AFFD73BEA233B510D37D13193801D94E5148D3EC4159653BC
Malicious:	false
Reputation:	unknown
Preview:	.....GDEF.m.v.....GPOSB..... ..KzGSUB..B..P...]@OS/2 |.....`cmapL.....<..d.cvt NY....l....&fpgmb/....J.....gasp.....l.....glyf.B....$..S(head0R...fL...6hhea...X..f ....$hmtx:4.7..f...-.loca.>b....`..-.maxp.t..... name(.2X...<....post}.....4...xprepldhL..X.....I...K.....J...L.Z...].f.. .i.w...z.|...~.....(...*.,.../.0...2.5...8.;...=.N...P.P...R.V...X.q...s.s...u.v...x.y...{..... ...).)..... .0.3...5.5...:.:...<.?...A.C...K.K...M.M...Q.Q...S.T...[.[...].]...j.k...p.q.....%.%...).D...G.I...U.V...Z.b...d.u...x.z.....P.P ...i.....`...c.....I...#

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraBoldItalic.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 38 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter ExtraBoldItalic4.000;git-a52131595;RSMS;Inter-Extr
Category:	dropped
Size (bytes):	422904
Entropy (8bit):	6.1847822896243585
Encrypted:	false
SSDEEP:	12288:EMPffL+f3H4g6WqgDVHqLhDj+359q7z8O8:1khq9Dj+3vrO8

MD5:	CDEF819CDB20F81FEB8A2ABDEBE9CDA0
SHA1:	EB61A79464DE3932A2D892BF50AD0270BE5791E2
SHA-256:	6A2CF89B061033C76C3CD7451113F3D8D29CE2C2E80B273FD60F9474E3927CBC
SHA-512:	04DE3B444603887E130870DC9FFF2F6798D737EA77A376C0A6D62C9114709F7891C95FA1BDDAB70FF055EBF127C6584CAECC594659F2E8596E72DA9D62D625E
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOS..\>.....I(GSUB*|.@..N0..[.OS/2 }..... ...`cmap^.....d.cvt N:....c....&fpgmb/....d.....gasp.....c.....glyf.....t8head0h....H...6hhea...x.....$hmt x.)....-$loca..MD.....-(maxp.D..... name+i1.....postz..... ..}.prepldhL..r.....*...;.....:...>.H...J.X...[.]..._.`...b.y...{... ...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.|...~..... ...".$...,,..... ..2.2...4.5...<.<...>.>...K.L...Q.R.....%...(.*...6.7...;.C...E.V...Y.[...g.h...m.n...q.s.....1.1...J.d...f.g...n.n...p.p..... .....A...D.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraLight.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 39 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter ExtraLightRegular4.000;git-a521315 95;RSMS;Inter-Ex
Category:	dropped
Size (bytes):	409996
Entropy (8bit):	6.169466966393304
Encrypted:	false
SSDEEP:	12288:XmzU22mZrPziKScOkpPSb+sv9wKKpuLpuSZAoM8:yiKcFyKK9SZ7M8
MD5:	B7E44012C53F3BCBF154C7C4784FCC14
SHA1:	101ABFE1C234D9E29504A55C7B5911F7E20E9425
SHA-256:	944F65A7C6CDA135C370559E9D7347BFDD45A579FE4DD1EF8BA5BC679BCD961D
SHA-512:	67808D6BDAFE9BCF5576DF234C93611BC827D868DD9F0D064E801DDA5EFE67883637746458B3A0E51B4B394913C3AC47F56C5C055B3FF013ABEBB66EC9A771 F
Malicious:	false
Reputation:	unknown
Preview:	.....GDEF.m.v.....GPOS{..... ..<^GSUB..B..A...]@OS/2.$.....`cmapL..... ..d.cvt D.....1\...&fpgmb/....2.....gasp.....1T....glyf.I.....I.head1....M....6hhea.....N ...$hmtx .....ND..-.loca.M.x..{...-.maxp.t..... name+.3.....post}F.....xprepldhL..@.....I...K.....J...L.Z...].f...i.w...z .|...~.....(...*,.../.0...2.5...8.;,..=.N...P.P...R.V...X.q...s.s...u.v...x.y...{..... ...).)..... .0.3...5 .5...:.:...<.?...A.C...K.K...M.M...Q.Q...S.T...[.[...].]...j.k...p.q.....%.%...).D...G.I...U.V...Z.b...d.u...x.z.....P.P...i..... .....`...c.....I...#

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraLightItalic.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 38 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter ExtraLightItalic4.000;git-a5213159 5;RSMS;Inter-Ext
Category:	dropped
Size (bytes):	415636
Entropy (8bit):	6.1951511440882685
Encrypted:	false
SSDEEP:	6144:327hgoK+yjo8AiWXWqSBCVUWR2kg4yODRVP8UPLumxDaAan+LHvKLMQyaInxFfmo:323K+tiqWqg3FkgdW3xDayLi78
MD5:	9E18D79ED628E74CA5E2EE3BFD6446BD
SHA1:	BF763C5CC7C91BFEC5E8E42499CA20AEF4C8B942
SHA-256:	BB5488DEFD018CF6CEA85B431A40991F0AB8939C39025E835E809160DCD912A6
SHA-512:	35A128E169D7CBC551C0337D78996E2061F8165E1B61870634A1EE6715199507F5FA140177C8A821401EAA765FC16FCC73E0180A21004803F6FC69EF512737F3
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOS>.uG.....:.GSUB*|.@..?...[.OS/2.%.....`cmap^.....D..d.cvt D.....Gd...&fpgmb/....H.....gasp.....G\....glyf*#:].....f.head1....f....6hhea.w....g....$hmt xe2.{..g4..-$loca...d...X..-(maxp.D..... name-.3z.....postz[.<.....}.prepldhL..V.....*...;.....:...>.H...J.X...[.]..._.`...b.y... {...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.|...~..... ...".$...,,..... .2.2...4.5...<.<...>.>...K.L...Q.R.....%...(.*...6.7...;.C...E.V...Y.[...g.h...m.n...q.s.....1.1...J.d...f.g...n.n...p.p..... .....A...D.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Italic.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 34 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInterItalic4.000;git-a52131595;RSMS;Inter-ItalicInter It
Category:	dropped
Size (bytes):	412848
Entropy (8bit):	6.2017904291058406
Encrypted:	false
SSDEEP:	12288:C2vSKsOi+1iqWqgfYs0S2S7vWAlcBJPH8:1PqIS2S7v3lcB98

MD5:	118ABBE34A2979B66D6838805C56B7CD
SHA1:	7F320CB81660FC6DFF9CC5751F8FCC0134847C77
SHA-256:	D054D998AE12BE33820B100E0ED3923D513FA5C79C6D4E7CA1953AFEB262EA9B
SHA-512:	5BCAD4A03CED2CE76C5EBF78CD2C1328A4EE27019807F56A48BF8A0F936C57F351F10726C176952F0CF08776A5CE53D34C14D6A848925BE2789408A61678F38
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOS.}.....7.GSUB*|.@..<...[.OS/2.....`cmap^.....d.cvt H.6..<....&fpgmb/....=.....gasp.....<x....glyf....._Lhead0..i..\....6hhea.?....]....$hmtxF)...],..-$loca.k6....P..-(maxp.D.....x... name.....>postzz.{.....}.prepldhL..K.....*...;.....;...>.H...J.X...[.]..._.`...b.y...{..... ...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.\...~..... ...".$...,.....2.2 ...4.5...<.<...>.>...K.L...Q.R.....%...(.*...6.7...;.C...E.V...Y.[...g.h...m.n...q.s.....1.1...J.d...f.g...n.n...p.p..... .....A...D.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.609503436410413
TrID:	• Win32 Executable (generic) a (10002005/4) 98.04% • Inno Setup installer (109748/4) 1.08% • InstallShield setup (43055/19) 0.42% • Win32 EXE PECompact compressed (generic) (41571/9) 0.41% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe
File size:	2'182'176 bytes
MD5:	dbb69ee00786bed3e12a04518e0f469a
SHA1:	40a82d88b06e6be8ba82fab34b4a29305466202a
SHA256:	dbc32537a29f5eba5406aa3f2ae409eb52ea904e76c19a74bfb480a8c8c63d69
SHA512:	e367614faeebe4af063634b911c3591c7c5b0e8c07a843753d809ce27c050b298ec5d1777ab2aa7c194810a45e4788ea98e93bf5b053beb375f8cc5a65cbcfae
SSDEEP:	24576:Y7FUDowAyrTVE3U5F/E3dwMzD3mseUwgjvKwX901all4qKxKic6QL3E2vVsjECUG:YBuZrEU8FTleUTKae2KIy029s4C1eH92
TLSH:	4CA5DF3FF268A13EC5AA1B3205B39310997BBA51A81A8C1F47FC344DCF765601E3B656
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	0c0c2d33ceec80aa

Static PE Info

General

Entrypoint:	0x4b5eec
Entrypoint Section:	.itext
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x63ECF218 [Wed Feb 15 14:54:16 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	e569e6f445d32ba23766ad67d1e3787f

Authenticode Signature	
Signature Valid:	**true**
Signature Issuer:	CN=GlobalSign GCC R45 CodeSigning CA 2020, O=GlobalSign nv-sa, C=BE
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 22/09/2023 15:18:31 03/12/2024 14:05:00
Subject Chain	• CN=OOO NBZ, O=OOO NBZ, L=Saint Petersburg, S=Saint Petersburg, C=RU
Version:	3
Thumbprint MD5:	644D93EB2A924788DC9F5A261B15A128
Thumbprint SHA-1:	8FF463CEC205068C449EBE08BC5EADB1E8BEF78D
Thumbprint SHA-256:	A0C6E99ECA1E36FBCEE4434A33A8862414BE13C68E7464DAE8CB84914EEF564E
Serial:	01181B5DC7EF7467C6035C60

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
add esp, FFFFFFA4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-3Ch], eax
mov dword ptr [ebp-40h], eax
mov dword ptr [ebp-5Ch], eax
mov dword ptr [ebp-30h], eax
mov dword ptr [ebp-38h], eax
mov dword ptr [ebp-34h], eax
mov dword ptr [ebp-2Ch], eax
mov dword ptr [ebp-28h], eax
mov dword ptr [ebp-14h], eax
mov eax, 004B14B8h
call 00007F16BC7F50F5h
xor eax, eax
push ebp
push 004B65E2h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 004B659Eh
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [004BE634h]
call 00007F16BC897BE7h
call 00007F16BC89773Ah
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007F16BC80AB94h
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D84h
call 00007F16BC7EFCE7h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [004C1D84h]
mov dl, 01h
mov eax, dword ptr [004238ECh]
call 00007F16BC80BD17h

Instruction
mov dword ptr [004C1D88h], eax
xor edx, edx
push ebp
push 004B654Ah
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007F16BC897C6Fh
mov dword ptr [004C1D90h], eax
mov eax, dword ptr [004C1D90h]
cmp dword ptr [eax+0Ch], 01h
jne 00007F16BC89DE8Ah
mov eax, dword ptr [004C1D90h]
mov edx, 00000028h
call 00007F16BC80C60Ch
mov edx, dword ptr [004C1D90h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc4000	0x9a	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2000	0xfdc	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc7000	0x11000	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x210900	0x4320	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc6000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xc22f4	0x254	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xc3000	0x1a4	.didata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb39e4	0xb3a00	43af0a9476ca224d8e8461f1e22c94da	False	0.34525867693110646	data	6.357635049994181	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0xb5000	0x1688	0x1800	185e04b9a1f554e31f7f848515dc890c	False	0.54443359375	data	5.971425428435973	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xb7000	0x37a4	0x3800	cab2107c933b696aa5cf0cc6c3fd3980	False	0.36097935267857145	data	5.048648594372454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0xbb000	0x6de8	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xc2000	0xfdc	0x1000	e7d1635e2624b124cfdce6c360ac21cd	False	0.3798828125	data	5.029087481102678	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.didata	0xc3000	0x1a4	0x200	8ced971d8a7705c98b173e255d8c9aa7	False	0.345703125	data	2.7509822285969876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0xc4000	0x9a	0x200	8d4e1e508031afe235bf121c80fd7d5f	False	0.2578125	data	1.877162954504408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0xc5000	0x18	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xc6000	0x5d	0x200	8f2f090acd9622c88a6a852e72f94e96	False	0.189453125	data	1.3838943752217987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc7000	0x11000	0x11000	7f89b554871894884a2a46b5f7d43d5a	False	0.18597771139705882	data	3.6934546558404633	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0xc7678	0xa68	Device independent bitmap graphic, 64 x 128 x 4, image size 2048	English	United States	0.1174924924924925
RT_ICON	0xc80e0	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States	0.15792682926829268
RT_ICON	0xc8748	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States	0.23387096774193547
RT_ICON	0xc8a30	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States	0.39864864864864863
RT_ICON	0xc8b58	0x1628	Device independent bitmap graphic, 64 x 128 x 8, image size 4096, 256 important colors	English	United States	0.08339210155148095
RT_ICON	0xca180	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States	0.1023454157782516
RT_ICON	0xcb028	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States	0.10649819494584838
RT_ICON	0xcb8d0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States	0.10838150289017341
RT_ICON	0xcbe38	0x12e5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States	0.8712011577424024
RT_ICON	0xcd120	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States	0.05668398677373642
RT_ICON	0xd1348	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States	0.08475103734439834
RT_ICON	0xd38f0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States	0.09920262664165103
RT_ICON	0xd4998	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States	0.2047872340425532
RT_STRING	0xd4e00	0x360	data			0.34375
RT_STRING	0xd5160	0x260	data			0.3256578947368421
RT_STRING	0xd53c0	0x45c	data			0.4068100358422939
RT_STRING	0xd581c	0x40c	data			0.3754826254826255
RT_STRING	0xd5c28	0x2d4	data			0.39226519337016574
RT_STRING	0xd5efc	0xb8	data			0.6467391304347826
RT_STRING	0xd5fb4	0x9c	data			0.6410256410256411
RT_STRING	0xd6050	0x374	data			0.4230769230769231
RT_STRING	0xd63c4	0x398	data			0.3358695652173913
RT_STRING	0xd675c	0x368	data			0.3795871559633027
RT_STRING	0xd6ac4	0x2a4	data			0.4275147928994083
RT_RCDATA	0xd6d68	0x10	data			1.5
RT_RCDATA	0xd6d78	0x2c4	data			0.6384180790960452
RT_RCDATA	0xd703c	0x2c	data			1.2045454545454546
RT_GROUP_ICON	0xd7068	0xbc	data	English	United States	0.6170212765957447
RT_VERSION	0xd7124	0x584	data	English	United States	0.26345609065155806

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_MANIFEST	0xd76a8	0x7a8	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.3377551020408163

Imports

DLL	Import
kernel32.dll	GetACP, GetExitCodeProcess, LocalFree, CloseHandle, SizeofResource, VirtualProtect, VirtualFree, GetFullPathNameW, ExitProcess, HeapAlloc, GetCPInfoExW, RtlUnwind, GetCPInfo, GetStdHandle, GetModuleHandleW, FreeLibrary, HeapDestroy, ReadFile, CreateProcessW, GetLastError, GetModuleFileNameW, SetLastError, FindResourceW, CreateThread, CompareStringW, LoadLibraryA, ResetEvent, GetVersion, RaiseException, FormatMessageW, SwitchToThread, GetExitCodeThread, GetCurrentThread, LoadLibraryExW, LockResource, GetCurrentThreadId, UnhandledExceptionFilter, VirtualQuery, VirtualQueryEx, Sleep, EnterCriticalSection, SetFilePointer, LoadResource, SuspendThread, GetTickCount, GetFileSize, GetStartupInfoW, GetFileAttributesW, InitializeCriticalSection, GetSystemWindowsDirectoryW, GetThreadPriority, SetThreadPriority, GetCurrentProcess, VirtualAlloc, GetSystemInfo, GetCommandLineW, LeaveCriticalSection, GetProcAddress, ResumeThread, GetVersionExW, VerifyVersionInfoW, HeapCreate, GetWindowsDirectoryW, VerSetConditionMask, GetDiskFreeSpaceW, FindFirstFileW, GetUserDefaultUILanguage, lstrlenW, QueryPerformanceCounter, SetEndOfFile, HeapFree, WideCharToMultiByte, FindClose, MultiByteToWideChar, LoadLibraryW, SetEvent, CreateFileW, GetLocaleInfoW, GetSystemDirectoryW, DeleteFileW, GetLocalTime, GetEnvironmentVariableW, WaitForSingleObject, WriteFile, ExitThread, DeleteCriticalSection, TlsGetValue, GetDateFormatW, SetErrorMode, IsValidLocale, TlsSetValue, CreateDirectoryW, GetSystemDefaultUILanguage, EnumCalendarInfoW, LocalAlloc, GetUserDefaultLangID, RemoveDirectoryW, CreateEventW, SetThreadLocale, GetThreadLocale
comctl32.dll	InitCommonControls
version.dll	GetFileVersionInfoSizeW, VerQueryValueW, GetFileVersionInfoW
user32.dll	CreateWindowExW, TranslateMessage, CharLowerBuffW, CallWindowProcW, CharUpperW, PeekMessageW, GetSystemMetrics, SetWindowLongW, MessageBoxW, DestroyWindow, CharUpperBuffW, CharNextW, MsgWaitForMultipleObjects, LoadStringW, ExitWindowsEx, DispatchMessageW
oleaut32.dll	SysAllocStringLen, SafeArrayPtrOfIndex, VariantCopy, SafeArrayGetLBound, SafeArrayGetUBound, VariantInit, VariantClear, SysFreeString, SysReAllocStringLen, VariantChangeType, SafeArrayCreate
netapi32.dll	NetWkstaGetInfo, NetApiBufferFree
advapi32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorW, RegQueryValueExW, AdjustTokenPrivileges, GetTokenInformation, ConvertSidToStringSidW, LookupPrivilegeValueW, RegCloseKey, OpenProcessToken, RegOpenKeyExW

Exports

Name	Ordinal	Address
TMethodImplementationIntercept	3	0x4541a8
__dbk_fcall_wrapper	2	0x40d0a0
dbkFCallWrapperAddr	1	0x4be63c

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

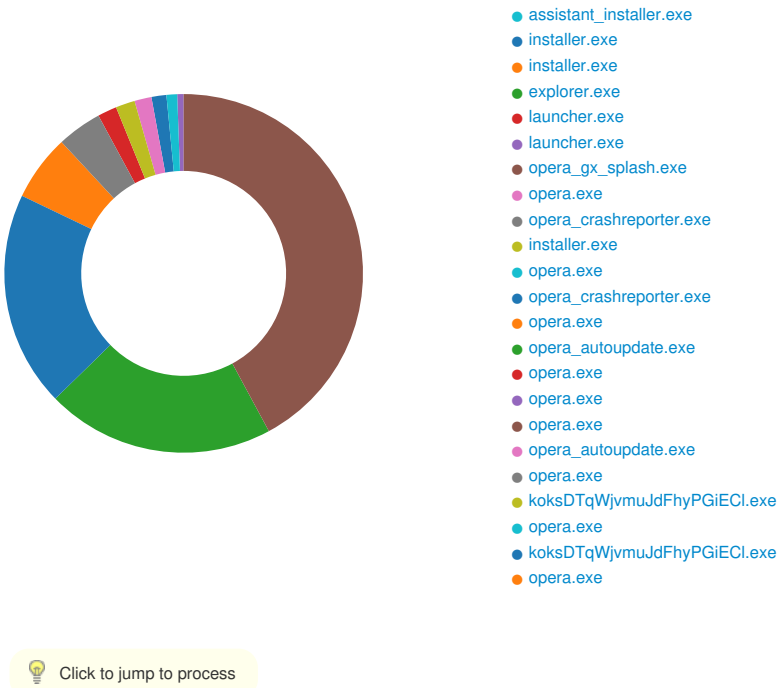
Network Behavior

Skipped network analysis since the amount of network traffic is too extensive. Please download the PCAP and check manually.

Statistics

Behavior

- SecuriteInfo.com.Adware.Elementa…
- SecuriteInfo.com.Adware.Elementa…
- OperaGXSetup.exe
- OperaGXSetup.exe
- OperaGXSetup.exe
- OperaGXSetup.exe
- OperaGXSetup.exe
- Opera_GX_assistant_73.0.3856.38…
- assistant_installer.exe



System Behavior

Analysis Process: SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe PID: 6512, Parent PID: 1028

General

Target ID:	0
Start time:	19:18:48
Start date:	29/03/2024
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe"
Imagebase:	0x400000
File size:	2'182'176 bytes
MD5 hash:	DBB69EE00786BED3E12A04518E0F469A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-TG3DC.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4AF02B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-TG3DC.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	423F32	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-TG3DC.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp	success or wait	1	4272D8	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-TG3DC.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp	0	3199488	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	424058	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	64	success or wait	1	423FBC	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	4	success or wait	2	423FBC	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	4	success or wait	2	423FBC	ReadFile

Analysis Process: SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp PID: **5996**, Parent PID: **6512**

General

Target ID:	1
Start time:	19:18:48
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-TG3DC.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-TG3DC.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp" /SL5="$1043A,1055917,832512,C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe"
Imagebase:	0x400000
File size:	3'199'488 bytes
MD5 hash:	668D5368DEF8B65631C43EECBD50EA48
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	60D5EB	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp_isetup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6ADA30	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	423762	CreateFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaLib.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5CC3DE	CreateFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\CommonConfig_en.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5CC3DE	CreateFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\Config.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5CC3DE	CreateFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\license.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5CC3DE	CreateFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\is-T2PA3.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5CC3DE	CreateFileW
C:\Users\user\Desktop\OperaGX-temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	60C33A	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\CommonConfig_en.json	success or wait	3	60C4D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\license.txt	success or wait	1	60C4D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaLib.dll	success or wait	1	60C4D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp_isetup_setup64.tmp	success or wait	1	60C4D0	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\is-T2PA3.tmp	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe	success or wait	1	60C857	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp_isetup_setup64.tmp	0	6144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e fd fd fd 1a fd fd fd 1a fd fd fd 1a fd fd fd 6c 07 fd fd 17 fd fd fd 1a fd fd fd 02 fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 52 69 63 68 1a fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 05 00 60 1c 52 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 0e 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$^l=\=\=\RichPE dR#	success or wait	1	4237AD	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaLib.dll	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2f 3c fd fd 6b 5d fd fd 6b 5d fd fd 6b 5d fd fd 20 25 fd fd 66 5d fd fd 20 25 fd fd fd 5d fd fd 20 25 fd fd 7e 5d fd fd fd fd 58 fd 6f 5d fd fd fd 21 fd 7a 5d fd fd fd 26 fd 72 5d fd fd fd 20 fd 3a 5d fd fd 6b 5d fd fd fd 5d fd fd 20 25 fd fd 7a 5d fd fd fd fd 45 fd 2a 5d fd fd fd ec fd 6f 5d fd fd fd e5 fd 6a 5d fd fd fd fd 5a fd 6a 5d fd fd fd e7 fd 6a 5d fd	MZ@!L!This program cannot be run in DOS mode.$/<k]k]k] %f] %] %~]Xo]z]r]:]k]] %z]E*]o]j]Zj]j]	success or wait	8	5CC538	WriteFile
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\CommonConfig_en.json	0	17934	7b 00 0d 00 0a 00 20 00 20 00 20 00 22 00 6f 00 66 00 66 00 65 00 72 00 73 00 22 00 3a 00 5b 00 20 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 7b 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 22 00 6e 00 61 00 6d 00 65 00 22 00 3a 00 20 00 22 00 6f 00 70 00 65 00 72 00 61 00 22 00 2c 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 22 00 74 00 79 00 70 00 65 00 22 00 3a 00 20 00 22 00 73 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 22 00 2c 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 22 00 69 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 4f 00 6e 00 6c 00 79 00 41 00 74 00 45 00 78 00 69 00 74 00 22 00 3a 00 20 00 74 00 72 00 75 00 65 00 2c 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 22 00 63 00 6f 00 6e 00 64 00 69 00 74 00 69 00 6f	{ "offers":[{ "name": "opera", "type": "standard", "installOnlyAtExit": true, "conditio	success or wait	1	5CC538	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\Config.json	0	25070	7b 00 0d 00 0a 00 20 00 20 00 20 00 20 00 22 00 63 00 6f 00 6d 00 6d 00 65 00 6e 00 74 00 73 00 22 00 3a 00 7b 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 22 00 74 00 61 00 72 00 67 00 65 00 74 00 41 00 70 00 70 00 22 00 3a 00 22 00 4f 00 70 00 65 00 72 00 61 00 47 00 58 00 22 00 2c 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 22 00 74 00 61 00 72 00 67 00 65 00 74 00 41 00 70 00 70 00 55 00 72 00 6c 00 22 00 3a 00 22 00 68 00 74 00 74 00 70 00 73 00 3a 00 2f 00 2f 00 74 00 72 00 79 00 2e 00 6f 00 70 00 65 00 72 00 61 00 2e 00 63 00 6f 00 6d 00 2f 00 37 00 32 00 54 00 52 00 38 00 52 00 37 00 2f 00 4b 00 4c 00 52 00 4c 00 35 00 37 00 39 00 2f 00 3f 00 73 00 75 00 62 00 31 00 3d 00 73 00 65 00 74 00 75 00 70 00 69 00 6f	{ "comments":{ "targetApp":"OperaGX", "targ etAppUrl":"https://try.opera.c om/72TR8R7/KLRL579/?sub1=setupio	success or wait	1	5CC538	WriteFile
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\license.txt	0	11490	45 6e 64 20 55 73 65 72 20 4c 69 63 65 6e 73 65 20 41 67 72 65 65 6d 65 6e 74 0d 0a 4f 70 65 72 61 20 66 6f 72 20 43 6f 6d 70 75 74 65 72 73 0d 0a 4c 61 73 74 20 75 70 64 61 74 65 64 3a 20 4f 63 74 6f 62 65 72 20 31 36 2c 20 32 30 32 30 0d 0a 0d 0a 54 68 69 73 20 65 6e 64 20 75 73 65 72 20 6c 69 63 65 6e 73 65 20 61 67 72 65 65 6d 65 6e 74 20 28 22 45 55 4c 41 22 29 20 67 6f 76 65 72 6e 73 20 79 6f 75 72 20 64 6f 77 6e 6c 6f 61 64 20 61 6e 64 2f 6f 72 20 75 73 65 20 6f 66 20 74 68 65 20 65 78 65 63 75 74 61 62 6c 65 20 63 6f 64 65 20 66 6f 72 20 74 68 65 20 4f 70 65 72 61 20 66 6f 72 20 43 6f 6d 70 75 74 65 72 73 20 64 65 73 6b 74 6f 70 20 73 6f 66 74 77 61 72 65 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 69 6e 63 6c 75 64 69 6e 67 20 61 6e 79 20 75 70 64	End User License AgreementOpera for ComputersLast updated: October 16, 2020This end user license agreement ("EULA") governs your download and/or use of the executable code for the Opera for Computers desktop software application, including any upd	success or wait	1	5CC538	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\is-T2PA3.tmp	0	3802	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 03 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 0e 00 00 50 36 00 00 40 00 00 00 60 25 00 70 fd 5b 00 00 70 25 00 00 fd 5b 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 00 5c 00 00 02 00 00 fd fd 36 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 fd fd 5b 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PELf"P6@`%p[p%[@\6@[	success or wait	724	423819	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	64	success or wait	1	5CC468	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	4	success or wait	2	5CC468	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	4	success or wait	2	5CC468	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	4	success or wait	1	5CC468	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	5	success or wait	2	5CC468	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	65536	success or wait	3	5CC468	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	4	success or wait	2	5CC468	ReadFile
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\CommonConfig_en.json	0	17934	success or wait	1	5CC468	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe	0	5	success or wait	2	5CC468	ReadFile
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\Config.json	0	25070	success or wait	1	5CC468	ReadFile
C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\license.txt	0	11490	success or wait	1	5CC468	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: OperaGXSetup.exe

PID: **1396**, Parent PID: **5996**

General

Target ID:	3
Start time:	19:18:57
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe" --silent --allusers=0
Imagebase:	0x130000
File size:	3'581'600 bytes
MD5 hash:	3C5239C753641E08EA3C2080FBFD5D51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818577271396.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	132E97	CreateFileW
C:\Users\user\AppData\Roaming\Opera Software	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B92E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B92E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\attachments	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B92E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B9452FA	CreateFileW
C:\Users\user\AppData\Local\Temp\1396_1212474782	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BA31718	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BA3800F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\OperaGXSetup.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BA31C44	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B88A447	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B88A447	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B88A447	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B88A447	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B88A447	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B88A447	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B87D387	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B87D387	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B87D387	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B87D387	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B87D387	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B87D387	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\opera_package	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B88A58D	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\40f6a45c-4b5f-4090-9566-45e04e14d0f6.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8DBF4F	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\additional_file0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B88A58D	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\additional_file1.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B88A58D	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\resources	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DD0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\files_list	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8DD675	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\server_tracking_data	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8DD675	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\ready	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8DD675	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\pref_default_overrides	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B88A58D	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\installer_prefs_include.json.backup	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6BA31C44	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\fe8a43e6-64dd-43a0-981d-b680f4d5d831.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8DBF4F	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\b9f9efb4-84f6-4d94-bf31-8ee44449c69d.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8DBF4F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\OperaGXSetup.exe	success or wait	1	6B8DC3AF	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	success or wait	1	6B8DC3AF	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe	success or wait	1	6B8DDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\browser_assistant.exe	success or wait	1	6B8DDCFA	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\files_list	success or wait	1	6B8DDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\mojo_core.dll	success or wait	2	6B8DDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\opera_package	success or wait	1	6B8DDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818577271396.dll	success or wait	1	131979	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1396_1212474782	C:\Users\user\AppData\Local\Temp\.opera	success or wait	1	6BA31D33	MoveFileExW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\40f6a45c-4b5f-4090-9566-45e04e14d0f6.tmp	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\installer_prefs_include.json	success or wait	1	6B8DC60F	MoveFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\additional_file0.tmp	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	success or wait	1	6BA31D33	MoveFileExW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\additional_file1.tmp	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\resources\custom_partner_content.json	success or wait	1	6BA31D33	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818577271396.dll	0	5449120	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 0a 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 33 00 00 38 1f 00 00 00 00 00 fd 26 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 54 00 00 04 00 00 fd fd 53 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 72 fd 3b 00 6d 00 00 00 e0 3b 00 fd 01 00	MZx@x!L!This program cannot be run in DOS mode.$PELf"!38&TS@Ar;m;	success or wait	1	132F54	WriteFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	73 64 50 43 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 41 fd fd 6d 1a fd 4e fd 3c fd fd 47 48 fd fd	sdPC\AmN<GH	success or wait	1	6B9451DE	WriteFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	73 64 50 43 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 41 fd fd 6d 1a fd 4e fd 3c fd fd 47 48 fd fd	sdPC\AmN<GH	success or wait	1	6B9451DE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	0	105	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 35 33 29 5d 20 4f 70 65 72 61 20 47 58 20 69 6e 73 74 61 6c 6c 65 72 20 73 74 61 72 74 69 6e 67 20 2d 20 76 65 72 73 69 6f 6e 20 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 20 53 74 61 62 6c 65 0a	[0329/191858.055:INFO:installer_main.cc(453)] Opera GX installer starting - version 107.0.5045.79 Stable	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	105	149	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 35 36 29 5d 20 43 6f 6d 6d 61 6e 64 20 6c 69 6e 65 3a 20 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 73 2d 4e 4d 39 33 4b 2e 74 6d 70 5c 4f 70 65 72 61 47 58 53 65 74 75 70 2e 65 78 65 22 20 2d 2d 73 69 6c 65 6e 74 20 2d 2d 61 6c 6c 75 73 65 72 73 3d 30 0a	[0329/191858.055:INFO:installer_main.cc(456)] Command line: "C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe" --silent --allusers=0	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	254	58	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 37 38 29 5d 20 55 6e 69 6e 73 74 61 6c 6c 3a 30 0a	[0329/191858.055:INFO:installer_main.cc(478)] Uninstall:0	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	312	55	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 37 39 29 5d 20 53 69 6c 65 6e 74 3a 31 0a	[0329/191858.055:INFO:installer_main.cc(479)] Silent:1	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	367	63	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 30 29 5d 20 52 75 6e 20 49 6d 6d 65 64 69 61 74 65 6c 79 30 0a	[0329/191858.055:INFO:installer_main.cc(480)] Run Immediately0	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	430	55	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 32 29 5d 20 42 61 63 6b 65 6e 64 30 0a	[0329/191858.055:INFO:installer_main.cc(482)] Backend0	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	485	62	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 33 29 5d 20 49 6e 73 69 64 65 20 70 61 63 6b 61 67 65 30 0a	[0329/191858.055:INFO:installer_main.cc(483)] Inside package0	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	547	59	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 34 29 5d 20 41 75 74 6f 75 70 64 61 74 65 3a 30 0a	[0329/191858.055:INFO:installer_main.cc(484)] Autoupdate:0	success or wait	1	6B8ED6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	606	67	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 70 61 79 6c 6f 61 64 5f 6d 61 6e 61 67 65 72 5f 69 6d 70 6c 2e 63 63 28 39 37 29 5d 20 52 65 61 64 69 6e 67 20 50 61 79 6c 6f 61 64 0a	[0329/191858.055:INFO:payload_manager_impl.cc(97)] Reading Payload	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	673	822	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 36 31 30 29 5d 20 54 72 61 63 6b 69 6e 67 20 64 61 74 61 3a 20 5a 57 5a 68 4f 44 52 6b 4d 44 4d 78 4e 57 4d 30 4e 44 4e 6c 59 6a 55 34 5a 44 56 6a 4d 32 45 32 5a 44 67 35 59 7a 67 79 4e 7a 41 34 5a 6a 49 79 4f 57 51 7a 4e 7a 67 78 4e 6d 45 77 59 6a 42 68 5a 44 46 6a 4e 7a 41 77 4d 54 6b 35 4e 57 4e 6c 4f 54 5a 69 5a 44 70 37 49 6d 4e 76 64 57 35 30 63 6e 6b 69 4f 69 4a 56 55 79 49 73 49 6d 56 6b 61 58 52 70 62 32 34 69 4f 69 4a 7a 64 47 51 74 4d 53 49 73 49 6d 6c 75 63 33 52 68 62 47 78 6c 63 6c 39 75 59 57 31 6c 49 6a 6f 69 54 33 42 6c 63 6d 46 48 57 46 4e 6c 64 48 56 77 4c 6d 56 34 5a 53 49 73 49 6e 42 79 62 32 52 31 59 33 51 69 4f 69	[0329/191858.055:INFO:installer_main.cc(610)] Tracking data: ZWZhODRkMDMxNWM0NDNlYjU4ZDVjM2E2ZDg5YzgyNzA4ZjIyOWQzNzgxNmEwYjBhZDFjNzAwMTk5NWNlOTZiZDp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOi	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	1495	88	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 73 65 74 74 69 6e 67 73 5f 69 6d 70 6c 2e 63 63 28 37 38 35 29 5d 20 46 6f 75 6e 64 20 33 20 70 61 74 68 73 20 66 6f 72 20 73 74 61 6e 64 61 6c 6f 6e 65 20 69 6e 73 74 61 6c 6c 20 6d 6f 64 65 2e 0a	[0329/191858.055:INFO:settings_impl.cc(785)] Found 3 paths for standalone install mode.	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	1583	100	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 72 65 73 6f 75 72 63 65 5f 6c 31 30 6e 5f 68 61 6e 64 6c 65 72 2e 63 63 28 31 31 33 29 5d 20 4c 61 6e 67 75 61 67 65 20 6e 6f 74 20 69 6e 20 74 68 65 20 61 76 61 69 6c 61 62 6c 65 20 6c 61 6e 67 75 61 67 65 73 20 6c 69 73 74 3a 20 0a	[0329/191858.055:INFO:resource_l10n_handler.cc(113)] Language not in the available languages list:	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	1683	103	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 30 35 35 3a 49 4e 46 4f 3a 72 65 73 6f 75 72 63 65 5f 6c 31 30 6e 5f 68 61 6e 64 6c 65 72 2e 63 63 28 31 31 39 29 5d 20 54 72 79 69 6e 67 20 6c 61 6e 67 75 61 67 65 20 66 72 6f 6d 20 73 79 73 74 65 6d 20 70 72 65 66 65 72 72 65 64 20 6c 69 73 74 3a 20 65 6e 2d 47 42 0a	[0329/191858.055:INFO:resource_l10n_handler.cc(119)] Trying language from system preferred list: en-GB	success or wait	1	6B8ED6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\OperaGXSetup.exe	0	524288	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 03 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 0e 00 00 50 36 00 00 40 00 00 00 60 25 00 70 fd 5b 00 00 70 25 00 00 fd 5b 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 00 00 5c 00 00 02 00 00 fd fd 36 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 5b 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PELf"P6@`%p[p%[@\6@[	success or wait	7	6BA31C44	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	1786	146	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 33 30 3a 49 4e 46 4f 3a 73 63 6f 70 65 64 5f 64 6f 77 6e 6c 6f 61 64 5f 66 6f 6c 64 65 72 2e 63 63 28 35 39 29 5d 20 49 6e 73 74 61 6c 6c 65 72 20 64 6f 77 6e 6c 6f 61 64 20 66 6f 6c 64 65 72 3a 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 2e 6f 70 65 72 61 5c 4f 70 65 72 61 20 47 58 20 49 6e 73 74 61 6c 6c 65 72 20 54 65 6d 70 0a	[0329/191858.430:INFO:scoped_download_folder.cc(59)] Installer download folder: C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	1932	114	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 73 65 74 74 69 6e 67 73 5f 69 6d 70 6c 2e 63 63 28 31 33 32 37 29 5d 20 49 6e 73 74 61 6c 6c 20 66 6f 6c 64 65 72 20 73 65 74 3a 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 50 72 6f 67 72 61 6d 73 5c 4f 70 65 72 61 20 47 58 0a	[0329/191858.446:INFO:settings_impl.cc(1327)] Install folder set: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	2046	59	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 73 65 74 74 69 6e 67 73 5f 69 6d 70 6c 2e 63 63 28 31 33 38 32 29 5d 20 4f 70 65 72 61 74 69 6f 6e 3a 20 31 0a	[0329/191858.446:INFO:settings_impl.cc(1382)] Operation: 1	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	2105	88	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 6d 61 69 6e 5f 70 72 6f 63 65 73 73 5f 69 6e 73 74 61 6c 6c 65 72 5f 72 75 6e 6e 65 72 5f 69 6d 70 6c 2e 63 63 28 36 38 29 5d 20 42 65 67 69 6e 6e 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 0a	[0329/191858.446:INFO:main_process_installer_runner_impl.cc(68)] Beginning installation	success or wait	1	6B8ED6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	2193	1834	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 6d 61 69 6e 5f 70 72 6f 63 65 73 73 5f 69 6e 73 74 61 6c 6c 65 72 5f 72 75 6e 6e 65 72 5f 69 6d 70 6c 2e 63 63 28 31 39 31 29 5d 20 6c 61 75 6e 63 68 69 6e 67 20 69 6e 73 74 61 6c 6c 65 72 20 62 61 63 6b 65 6e 64 3a 20 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 73 2d 4e 4d 39 33 4b 2e 74 6d 70 5c 4f 70 65 72 61 47 58 53 65 74 75 70 2e 65 78 65 22 20 2d 2d 62 61 63 6b 65 6e 64 20 2d 2d 69 6e 73 74 61 6c 6c 20 2d 2d 69 6d 70 6f 72 74 2d 62 72 6f 77 73 65 72 2d 64 61 74 61 3d 30 20 2d 2d 65 6e 61 62 6c 65 2d 73 74 61 74 73 3d 31 20 2d 2d 65 6e 61 62 6c 65 2d 69 6e 73 74 61 6c 6c 65 72 2d 73 74 61 74 73 3d 31 20 2d 2d 63 6f 6e	[0329/191858.446:INFO:main_process_installer_runner_impl.cc(191)] launching installer backend: "C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe" --backend --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --con	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4027	113	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 33 33 38 29 5d 20 53 74 61 72 74 69 6e 67 20 64 6f 77 6e 6c 6f 61 64 20 66 72 6f 6d 20 68 74 74 70 73 3a 2f 2f 61 75 74 6f 75 70 64 61 74 65 2e 67 65 6f 2e 6f 70 65 72 61 2e 63 6f 6d 2f 67 65 6f 6c 6f 63 61 74 69 6f 6e 2f 0a	[0329/191858.446:INFO:wininet_impl.cc(338)] Starting download from https://autoupdate.geo.opera.com/geolocation/	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4140	66	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 37 35 35 29 5d 20 53 74 6f 70 70 69 6e 67 20 74 68 65 20 64 6f 77 6e 6c 6f 61 64 0a	[0329/191858.446:INFO:wininet_impl.cc(755)] Stopping the download	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4206	89	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 70 61 63 6b 61 67 65 5f 66 65 74 63 68 5f 73 65 71 75 65 6e 63 65 72 5f 69 6d 70 6c 2e 63 63 28 31 35 36 29 5d 20 53 74 61 72 74 69 6e 67 20 74 68 65 20 70 61 63 6b 61 67 65 20 66 65 74 63 68 65 72 0a	[0329/191858.446:INFO:package_fetch_sequencer_impl.cc(156)] Starting the package fetcher	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4295	99	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 70 61 63 6b 61 67 65 5f 6d 65 74 61 64 61 74 61 5f 72 65 74 72 69 65 76 65 72 5f 69 6d 70 6c 2e 63 63 28 33 33 33 29 5d 20 50 72 65 70 61 72 69 6e 67 20 74 6f 20 66 65 74 63 68 20 74 68 65 20 64 6f 77 6e 6c 6f 61 64 20 55 52 4c 0a	[0329/191858.446:INFO:package_metadata_retriever_impl.cc(333)] Preparing to fetch the download URL	success or wait	1	6B8ED6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4394	89	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 70 61 63 6b 61 67 65 5f 6d 65 74 61 64 61 74 61 5f 72 65 74 72 69 65 76 65 72 5f 69 6d 70 6c 2e 63 63 28 33 39 31 29 5d 20 46 65 74 63 68 69 6e 67 20 74 68 65 20 64 6f 77 6e 6c 6f 61 64 20 55 52 4c 0a	[0329/191858.446:INFO:package_metadata_retriever_impl.cc(391)] Fetching the download URL	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4483	138	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 34 34 36 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 33 33 38 29 5d 20 53 74 61 72 74 69 6e 67 20 64 6f 77 6e 6c 6f 61 64 20 66 72 6f 6d 20 68 74 74 70 73 3a 2f 2f 61 75 74 6f 75 70 64 61 74 65 2e 67 65 6f 2e 6f 70 65 72 61 2e 63 6f 6d 2f 76 35 2f 6e 65 74 69 6e 73 74 61 6c 6c 65 72 2f 67 78 2f 53 74 61 62 6c 65 2f 77 69 6e 64 6f 77 73 2f 78 36 34 0a	[0329/191858.446:INFO:wininet_impl.cc(338)] Starting download from https://autoupdate.geo.opera.com/v5/netinstaller/gx/Stable/windows/x64	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4621	71	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 34 33 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 36 31 31 29 5d 20 49 6e 69 74 69 61 6c 20 72 65 71 75 65 73 74 20 63 6f 6d 70 6c 65 74 69 6f 6e 0a	[0329/191859.243:INFO:wininet_impl.cc(611)] Initial request completion	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4692	135	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 34 33 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 36 33 35 29 5d 20 43 6f 75 6c 64 20 6e 6f 74 20 67 65 74 20 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 20 66 72 6f 6d 20 72 65 73 70 6f 6e 73 65 3a 20 45 72 72 6f 72 20 28 30 78 31 33 44 29 20 77 68 69 6c 65 20 72 65 74 72 69 65 76 69 6e 67 20 65 72 72 6f 72 2e 20 28 30 78 32 46 37 36 29 0a	[0329/191859.243:INFO:wininet_impl.cc(635)] Could not get Content-Length from response: Error (0x13D) while retrieving error. (0x2F76)	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4827	63	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 37 34 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 38 38 35 29 5d 20 44 6f 77 6e 6c 6f 61 64 20 63 6f 6d 70 6c 65 74 65 64 0a	[0329/191859.274:INFO:wininet_impl.cc(885)] Download completed	success or wait	1	6B8ED6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	4890	231	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 37 34 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 33 33 38 29 5d 20 53 74 61 72 74 69 6e 67 20 64 6f 77 6e 6c 6f 61 64 20 66 72 6f 6d 20 68 74 74 70 73 3a 2f 2f 66 65 61 74 75 72 65 73 2e 6f 70 65 72 61 2d 61 70 69 32 2e 63 6f 6d 2f 61 70 69 2f 76 32 2f 66 65 61 74 75 72 65 73 3f 63 6f 75 6e 74 72 79 3d 55 53 26 6c 61 6e 67 75 61 67 65 3d 65 6e 2d 47 42 26 75 75 69 64 3d 61 38 31 38 65 37 37 62 2d 31 37 65 34 2d 34 35 32 63 2d 39 31 39 64 2d 38 33 30 65 37 37 31 33 64 37 35 66 26 70 72 6f 64 75 63 74 3d 67 78 26 63 68 61 6e 6e 65 6c 3d 53 74 61 62 6c 65 26 76 65 72 73 69 6f 6e 3d 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 0a	[0329/191859.274:INFO:wininet_impl.cc(338)] Starting download from https://features.opera-api2.com/api/v2/features?country=US&language=en-GB&uuid=a818e77b-17e4-452c-919d-830e7713d75f&product=gx&channel=Stable&version=107.0.5045.79	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5121	71	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 39 30 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 36 31 31 29 5d 20 49 6e 69 74 69 61 6c 20 72 65 71 75 65 73 74 20 63 6f 6d 70 6c 65 74 69 6f 6e 0a	[0329/191859.290:INFO:wininet_impl.cc(611)] Initial request completion	success or wait	3	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5192	135	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 39 30 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 36 33 35 29 5d 20 43 6f 75 6c 64 20 6e 6f 74 20 67 65 74 20 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 20 66 72 6f 6d 20 72 65 73 70 6f 6e 73 65 3a 20 45 72 72 6f 72 20 28 30 78 31 33 44 29 20 77 68 69 6c 65 20 72 65 74 72 69 65 76 69 6e 67 20 65 72 72 6f 72 2e 20 28 30 78 32 46 37 36 29 0a	[0329/191859.290:INFO:wininet_impl.cc(635)] Could not get Content-Length from response: Error (0x13D) while retrieving error. (0x2F76)	success or wait	2	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5327	63	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 39 30 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 38 38 35 29 5d 20 44 6f 77 6e 6c 6f 61 64 20 63 6f 6d 70 6c 65 74 65 64 0a	[0329/191859.290:INFO:wininet_impl.cc(885)] Download completed	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5390	94	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 39 30 3a 49 4e 46 4f 3a 70 61 63 6b 61 67 65 5f 6d 65 74 61 64 61 74 61 5f 72 65 74 72 69 65 76 65 72 5f 69 6d 70 6c 2e 63 63 28 34 38 35 29 5d 20 46 65 74 63 68 69 6e 67 20 74 68 65 20 61 64 64 69 74 69 6f 6e 61 6c 20 63 6f 6e 66 69 67 0a	[0329/191859.290:INFO:package_metadata_retriever_impl.cc(485)] Fetching the additional config	success or wait	1	6B8ED6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5484	224	5b 30 33 32 39 2f 31 39 31 38 35 39 2e 32 39 30 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 33 33 38 29 5d 20 53 74 61 72 74 69 6e 67 20 64 6f 77 6e 6c 6f 61 64 20 66 72 6f 6d 20 68 74 74 70 73 3a 2f 2f 63 6f 6e 66 69 67 2e 67 78 2e 67 61 6d 65 73 2f 76 30 2f 63 6f 6e 66 69 67 3f 75 74 6d 5f 63 61 6d 70 61 69 67 6e 3d 50 57 4e 5f 55 53 5f 50 42 34 5f 33 37 34 32 26 75 74 6d 5f 6d 65 64 69 75 6d 3d 70 61 26 75 74 6d 5f 73 6f 75 72 63 65 3d 50 57 4e 67 61 6d 65 73 26 70 72 6f 64 75 63 74 3d 67 78 26 63 68 61 6e 6e 65 6c 3d 53 74 61 62 6c 65 26 63 6c 69 65 6e 74 3d 6e 65 74 69 6e 73 74 61 6c 6c 65 72 26 65 64 69 74 69 6f 6e 3d 73 74 64 2d 31 0a	[0329/191859.290:INFO:wininet_impl.cc(338)] Starting download from https://config.gx.games/v0/config?utm_campaign=PWN_US_PB4_3742&utm_medium=pa&utm_source=PWNgames&product=gx&channel=Stable&client=netinstaller&edition=std-1	success or wait	2	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5708	71	5b 30 33 32 39 2f 31 39 31 39 30 30 2e 30 34 30 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 36 31 31 29 5d 20 49 6e 69 74 69 61 6c 20 72 65 71 75 65 73 74 20 63 6f 6d 70 6c 65 74 69 6f 6e 0a	[0329/191900.040:INFO:wininet_impl.cc(611)] Initial request completion	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\T9RRWRNL\features[1].json	0	1024	7b 22 66 65 61 74 75 72 65 73 22 3a 7b 22 30 31 39 37 39 32 39 39 63 38 63 64 22 3a 7b 22 73 74 61 74 65 22 3a 22 65 6e 61 62 6c 65 64 22 7d 2c 22 31 33 65 30 32 35 66 36 34 62 64 36 22 3a 7b 22 73 74 61 74 65 22 3a 22 64 69 73 61 62 6c 65 64 22 7d 2c 22 31 33 65 65 61 66 38 35 31 64 61 37 22 3a 7b 22 73 74 61 74 65 22 3a 22 65 6e 61 62 6c 65 64 22 7d 2c 22 31 35 33 32 32 66 34 38 39 39 37 36 22 3a 7b 22 73 74 61 74 65 22 3a 22 65 6e 61 62 6c 65 64 22 7d 2c 22 31 61 64 36 39 62 30 30 37 63 65 35 22 3a 7b 22 73 74 61 74 65 22 3a 22 65 6e 61 62 6c 65 64 22 7d 2c 22 31 63 34 64 64 64 62 36 35 62 61 63 22 3a 7b 22 73 74 61 74 65 22 3a 22 65 6e 61 62 6c 65 64 22 7d 2c 22 31 64 32 34 64 63 65 62 39 33 37 61 22 3a 7b 22 73 74 61 74 65 22 3a 22 65 6e 61 62 6c 65	{"features":{"01979299c8cd":{"state":"enabled"},"13e025f64bd6":{"state":"disabled"},"13eeaf851da7":{"state":"enabled"},"15322f489976":{"state":"enabled"},"1ad69b007ce5":{"state":"enabled"},"1c4dddb65bac":{"state":"enabled"},"1d24dceb937a":{"state":"enable	success or wait	2	6B8892D3	InternetReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5779	63	5b 30 33 32 39 2f 31 39 31 39 30 30 2e 30 35 35 3a 49 4e 46 4f 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 38 38 35 29 5d 20 44 6f 77 6e 6c 6f 61 64 20 63 6f 6d 70 6c 65 74 65 64 0a	[0329/191900.055:INFO:wininet_impl.cc(885)] Download completed	success or wait	1	6B8ED6C3	WriteFile
unknown	unknown	99			invalid handle	1	6B9F2B21	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	5913	98	5b 30 33 32 39 2f 31 39 31 39 30 30 2e 33 30 35 3a 45 52 52 4f 52 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 39 34 32 29 5d 20 52 65 71 75 65 73 74 20 63 6f 6d 70 6c 65 74 65 64 20 77 69 74 68 20 61 6e 20 75 6e 65 78 70 65 63 74 65 64 20 48 54 54 50 20 73 74 61 74 75 73 20 34 30 34 0a	[0329/191900.305:ERROR:wininet_impl.cc(942)] Request completed with an unexpected HTTP status 404	success or wait	1	6B8ED6C3	WriteFile
unknown	unknown	62			invalid handle	1	6B9F2B21	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	6011	61	5b 30 33 32 39 2f 31 39 31 39 30 30 2e 33 30 35 3a 45 52 52 4f 52 3a 77 69 6e 69 6e 65 74 5f 69 6d 70 6c 2e 63 63 28 38 36 32 29 5d 20 44 6f 77 6e 6c 6f 61 64 20 66 61 69 6c 65 64 0a	[0329/191900.305:ERROR:wininet_impl.cc(862)] Download failed	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858040.log	6072	92	5b 30 33 32 39 2f 31 39 31 39 30 30 2e 33 30 35 3a 49 4e 46 4f 3a 6d 61 69 6e 5f 70 61 63 6b 61 67 65 5f 64 6f 77 6e 6c 6f 61 64 65 72 5f 69 6d 70 6c 2e 63 63 28 37 39 29 5d 20 50 72 65 70 61 72 69 6e 67 20 74 6f 20 66 65 74 63 68 20 74 68 65 20 69 6e 73 74 61 6c 6c 65 72 0a	[0329/191900.305:INFO:main_package_downloader_impl.cc(79)] Preparing to fetch the installer	success or wait	1	6B8ED6C3	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9C680Q69\Opera_GX_107.0.5045.79_Autoupdate_x64[1].exe	0	1018	4d 5a 60 00 01 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 52 65 71 75 69 72 65 20 57 69 6e 64 6f 77 73 0d 0a 24 50 45 00 00 4c 01 04 00 27 00 fd 50 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 08 00 00 28 01 00 00 46 00 00 00 00 00 00 fd 2d 01 00 00 10 00 00 00 40 01 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 0c 7a 08 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 fd 62 01 00 fd 00 00 00 00 fd 01 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 58 fd 79 08 fd 29 00	MZ`@`!L!Require Windows$PEL'P(F-@@zbXy)	success or wait	49723	6B8892D3	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\opera_package	0	1018	4d 5a 60 00 01 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 52 65 71 75 69 72 65 20 57 69 6e 64 6f 77 73 0d 0a 24 50 45 00 00 4c 01 04 00 27 00 fd 50 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 08 00 00 28 01 00 00 46 00 00 00 00 00 00 fd 2d 01 00 00 10 00 00 00 40 01 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 0c 7a 08 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 fd 62 01 00 fd 00 00 00 00 fd 01 00 fd 06 00 00 00 00 00 00 00 00 00 00 58 fd 79 08 fd 29 00	MZ`@`!L!Require Windows$PEL'P(F-@@zbXy)	success or wait	49972	6B88A646	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	end of file	1	6B945259	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	6B945259	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	6B945259	ReadFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	0	2048	pending	1	6B807EA4	ReadFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	0	2048	pending	247	6B807EA4	ReadFile
\pipe	0	1024	success or wait	1	6BA3046F	ReadFile
\pipe	0	1024	pipe broken	1	6BA3046F	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\installer_prefs_include.json	0	4096	success or wait	1	6B9EDF55	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\installer_prefs_include.json	0	4096	end of file	1	6B9EDF55	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: OperaGXSetup.exe PID: 3276, Parent PID: 1396

General

Target ID:	4
Start time:	19:18:57
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win32 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x2e4,0x2e8,0x2ec,0x2c0,0x2f0,0x6bb4623c,0x6bb46248,0x6bb46254
Imagebase:	0x130000

File size:	3'581'600 bytes
MD5 hash:	3C5239C753641E08EA3C2080FBFD5D51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818579403276.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	132E97	CreateFileW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B20E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B20E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\attachments	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B20E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\metadata	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B20E9B7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818579403276.dll	success or wait	1	131979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818579403276.dll	0	5449120	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 0a 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 33 00 00 38 1f 00 00 00 00 00 fd 26 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 54 00 00 04 00 00 fd fd 53 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 72 fd 3b 00 6d 00 00 00 e0 3b 00 fd 01 00	MZx@x!L!This program cannot be run in DOS mode.$PELf"!38&TS@Ar;m;	success or wait	1	132F54	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\crashpad_1396_VPWELDWQUGNWVGGM	0	36	success or wait	1	6B225259	ReadFile
\pipe\crashpad_1396_VPWELDWQUGNWVGGM	0	36	success or wait	1	6B225259	ReadFile

Analysis Process: OperaGXSetup.exe PID: **5068**, Parent PID: **1396**

General

Target ID:	5
Start time:	19:18:58
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\OperaGXSetup.exe" --version
Imagebase:	0x970000
File size:	3'581'600 bytes
MD5 hash:	3C5239C753641E08EA3C2080FBFD5D51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818582525068.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	972E97	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818582525068.dll	success or wait	1	971979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818582525068.dll	0	5449120	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 0a 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 33 00 00 38 1f 00 00 00 00 00 fd 26 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 54 00 00 04 00 00 fd fd 53 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 72 fd 3b 00 6d 00 00 00 e0 3b 00 fd 01 00	MZx@x!L!This program cannot be run in DOS mode.$PELf"!38&TS@Ar;m;	success or wait	1	972F54	WriteFile

Analysis Process: OperaGXSetup.exe PID: **652**, Parent PID: **1396**

General

Target ID:	6
Start time:	19:18:58
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe" --backend --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --consent-given=0 --general-interests=0 --general-location=0 --personalized-content=0 --personalized-ads=0 --launchopera=1 --installfolder="C:\Users\user\AppData\Local\Programs\Opera GX" --profile-folder --language=en-GB --singleprofile=0 --copyonly=0 --allusers=0 --setdefaultbrowser=1 --pintotaskbar=1 --pintostartmenu=1 --run-at-startup=1 --server-tracking-data=server_tracking_data --initial-pid=1396 --package-dir-prefix="C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_20240329191858" --session-guid=8ddbc8bc-ca9a-4c2b-a001-468713504759 --server-tracking-blob=NGFjMjBjZGM2OTE2N2RiNmJlYjJmY2M2YTBmZDdmMDY4ZjE3N2Y3OWFjNmExN2RhOTU2NGUyNWUyOTFkYjhlNjp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21lZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04MDVjOTQ2ZWM3YzU0NjgwYjM3ZjU4MmQ1OGRlMTgzMCZ1dG1fY29udGVudD0zNzQyX3NldHVwaW8iLCJzeXN0ZW0iOnsicGxhdGZvcm0iOnsiYXJjaCI6Ing4NI82NCIsIm9wc3lzIjoiV2luZG93cyIsIm9wc3lzLXZlcnNpb24iOiIxMCIsInBhY2thZ2UiOiJFWEUifX0sInRpbWVzdGFtcCI6IjE3MTE3MzYzMzYuNTM0NCIsInVzZXJhZ2VudCI6IklubXm8gU2V0dXAgNi4yLjIiLCJ1dG0iOnsiY2FtcGFpZ24iOiJQV05fVVNfUEI0XzM3NDIiLCJjb250ZW50IjoiMzc0MI9zZXR1cGIvIiwiaWQiOiI4MDVjOTQ2ZWM3YzU0NjgwYjM3ZjU4MmQ1OGRlMTgzMCIsIm1IZGl1bSI6InBhliwic291cmNlIjoiUFdOZ2FtZXMifSwidXVpZCI6ImFiN2E4MGUwLWY1MjItNDZjMy1iYzdlLWQxNzkzYjIwNDhlMiJ9 --silent --desktopshortcut=1 --wait-for-package --initial-proc-handle=7005000000000000
Imagebase:	0x130000
File size:	3'581'600 bytes
MD5 hash:	3C5239C753641E08EA3C2080FBFD5D51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_240329181858612652.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	132E97	CreateFileW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AC9E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AC9E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\attachments	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6AC9E67B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6ADA800F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\MEIPreload	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\standard_themes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC4D0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\107.0.5045.79.manifest	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-100.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-100_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-140.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-140_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-180.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-180_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-80.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-80_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-100.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-100_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-140.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-140_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-180.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-180_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-80.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-80_contrast-white.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\assistant_package	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\CUESDK.x64_2017.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\d3dcompiler_47.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxcompiler.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\dxil.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Black.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-BlackItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Bold.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-BoldItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraBold.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraBoldItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraLight.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ExtraLightItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Italic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Light.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-LightItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Medium.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-MediumItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Regular.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-SemiBold.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-SemiBoldItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Thin.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-ThinItalic.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\headless_command_resources.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\headless_lib_data.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\headless_lib_strings.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\icudtl.dat	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer_helper_64.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.visualelementsmanifest.xml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\libEGL.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\libGLESv2.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\bg.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\bn.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ca.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\cs.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\da.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\de.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\el.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\en-GB.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\en-US.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\es-419.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\es.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\fi.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\fil.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\fr.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\hi.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\hr.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\hu.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\id.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\it.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ja.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ko.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\lt.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\lv.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ms.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\nb.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\nl.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\pl.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\pt-BR.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\pt-PT.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ro.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ru.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\sk.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\sr.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\sv.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\sw.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ta.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\te.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\th.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\tr.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\uk.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\vi.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\zh-CN.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\zh-TW.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\MEIPreload\manifest.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\MEIPreload\preloaded_data.pb	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\mojo_core.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\notification_helper.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera.exe.sig	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera.visualelementsmanifest.xml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_100_percent.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_125_percent.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_150_percent.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_200_percent.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_250_percent.pak	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.licenses	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.version	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_browser.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_browser.dll.sig	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_crashreporter.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_elf.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_gx_splash.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Resources.pri	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\013E742B-287B-4228-A0B9-BD617E4E02A4.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\07593226-C5C5-438B-86BE-3F6361CD5B10.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\0CD5F3A0-8BF6-11E2-9E96-0800200C9A66.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\1AF2CDD0-8BF3-11E2-9E96-0800200C9A66.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\1CF37043-6733-479C-9086-7B21A2292DDA.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\2A3F5C20-8BF5-11E2-9E96-0800200C9A66.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\2F8F0E41-F521-45A4-9691-F664AFAFE67F.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\3B6191A0-8BF3-11E2-9E96-0800200C9A66.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\3BFDFA54-5DD6-4DFF-8B6C-C1715F306D6B.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\4C95ADC1-5FD9-449D-BC75-77CA217403AE.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\5BBBDD5B-EDC7-4168-9F5D-290AF826E716.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\66DD4BB6-A3BA-4B11-AF7A-F4BF23E073B2.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\6D3582E1-6013-429F-BB34-C75B90CDD1F8.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\76C397A8-9E8E-4706-8203-BD2878E9C618.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\8D754F20-8BF5-11E2-9E96-0800200C9A66.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\ab_tests.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\AD2FD2BD-0727-4AF7-8917-AAED8627ED47.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\automatic_search_engines.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\B478FE0C-0761-41C3-946F-CD1340356039.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\browser.js	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\C665D993-1B49-4C2E-962C-BEB19993BB86.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\CCCED631-6DA2-4060-9824-95737E64350C.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\CFCE84E5-9A95-4B3F-B8E4-3E98CF7EE6C5.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\CFD4BE41-4C6D-496A-ADDB-4095DFA1DD0E.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\continue_shopping.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\daily_wallpapers.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\default_partner_content.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\doh_providers.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\F3F34CBB-24FF-4830-9E87-1663E7A0A5EE.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\F98D4D4C-8AA7-4619-A1E7-AC89B24558DD.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\FDC2CCAB-E8F9-4620-91DD-B0B67285997C.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\FF57F01A-0718-44B7-8A1F-8B15BC33A50B.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\FFF3F819-B6CE-4DE6-B4E4-8E2618ABC0D9.ico	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\partner_speeddials.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\purchases-schemas.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\siteprefs.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\specific_keywords.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\standard_themes\default_dark_theme.zip	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\standard_themes\gx-1-classic-dark.zip	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\standard_themes\gx-1-classic-light.zip	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\standard_themes\gx-classic-dark.zip	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\standard_themes\gx-classic-light.zip	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\video_conference_popout.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\snapshot_blob.bin	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\v8_context_snapshot.bin	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\vk_swiftshader.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\vk_swiftshader_icd.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\vulkan-1.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\win10_share_handler.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\win8_importing.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC4BF4F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\done	success or wait	1	6AC4C3AF	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_240329181858612652.dll	success or wait	1	131979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_240329181858612652.dll	0	5449120	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 0a 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 33 00 00 38 1f 00 00 00 00 00 fd 26 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 54 00 00 04 00 00 fd fd 53 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 72 fd 3b 00 6d 00 00 00 e0 3b 00 fd 01 00	MZx@x!L!This program cannot be run in DOS mode.$PELf"!38&TS@Ar;m;	success or wait	1	132F54	WriteFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	73 64 50 43 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 41 fd fd 6d 1a fd 4e fd 3c fd fd 47 48 fd fd	sdPC\AmN<GH	success or wait	1	6ACB51DE	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	0	105	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 35 36 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 35 33 29 5d 20 4f 70 65 72 61 20 47 58 20 69 6e 73 74 61 6c 6c 65 72 20 73 74 61 72 74 69 6e 67 20 2d 20 76 65 72 73 69 6f 6e 20 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 20 53 74 61 62 6c 65 0a	[0329/191858.956:INFO:installer_main.cc(453)] Opera GX installer starting - version 107.0.5045.79 Stable	success or wait	1	6AC5D6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	105	1799	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 35 36 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 35 36 29 5d 20 43 6f 6d 6d 61 6e 64 20 6c 69 6e 65 3a 20 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 73 2d 4e 4d 39 33 4b 2e 74 6d 70 5c 4f 70 65 72 61 47 58 53 65 74 75 70 2e 65 78 65 22 20 2d 2d 62 61 63 6b 65 6e 64 20 2d 2d 69 6e 73 74 61 6c 6c 20 2d 2d 69 6d 70 6f 72 74 2d 62 72 6f 77 73 65 72 2d 64 61 74 61 3d 30 20 2d 2d 65 6e 61 62 6c 65 2d 73 74 61 74 73 3d 31 20 2d 2d 65 6e 61 62 6c 65 2d 69 6e 73 74 61 6c 6c 65 72 2d 73 74 61 74 73 3d 31 20 2d 2d 63 6f 6e 73 65 6e 74 2d 67 69 76 65 6e 3d 30 20 2d 2d 67 65 6e 65 72 61 6c 2d 69 6e 74 65 72 65 73 74 73 3d 30 20	[0329/191858.956:INFO:installer_main.cc(456)] Command line: "C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe" --backend --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --consent-given=0 --general-interests=0	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	1904	128	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 37 35 29 5d 20 49 6e 73 74 61 6c 6c 20 66 6f 6c 64 65 72 20 66 72 6f 6d 20 63 6f 6d 6d 61 6e 64 20 6c 69 6e 65 3a 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 50 72 6f 67 72 61 6d 73 5c 4f 70 65 72 61 20 47 58 0a	[0329/191858.971:INFO:installer_main.cc(475)] Install folder from command line: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2032	58	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 37 38 29 5d 20 55 6e 69 6e 73 74 61 6c 6c 3a 30 0a	[0329/191858.971:INFO:installer_main.cc(478)] Uninstall:0	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2090	55	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 37 39 29 5d 20 53 69 6c 65 6e 74 3a 31 0a	[0329/191858.971:INFO:installer_main.cc(479)] Silent:1	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2145	63	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 30 29 5d 20 52 75 6e 20 49 6d 6d 65 64 69 61 74 65 6c 79 30 0a	[0329/191858.971:INFO:installer_main.cc(480)] Run Immediately0	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2208	55	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 32 29 5d 20 42 61 63 6b 65 6e 64 31 0a	[0329/191858.971:INFO:installer_main.cc(482)] Backend1	success or wait	1	6AC5D6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2263	62	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 33 29 5d 20 49 6e 73 69 64 65 20 70 61 63 6b 61 67 65 30 0a	[0329/191858.971:INFO:installer_main.cc(483)] Inside package0	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2325	59	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 34 38 34 29 5d 20 41 75 74 6f 75 70 64 61 74 65 3a 30 0a	[0329/191858.971:INFO:installer_main.cc(484)] Autoupdate:0	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2384	67	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 70 61 79 6c 6f 61 64 5f 6d 61 6e 61 67 65 72 5f 69 6d 70 6c 2e 63 63 28 39 37 29 5d 20 52 65 61 64 69 6e 67 20 50 61 79 6c 6f 61 64 0a	[0329/191858.971:INFO:payload_manager_impl.cc(97)] Reading Payload	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	2451	822	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 36 31 30 29 5d 20 54 72 61 63 6b 69 6e 67 20 64 61 74 61 3a 20 5a 57 5a 68 4f 44 52 6b 4d 44 4d 78 4e 57 4d 30 4e 44 4e 6c 59 6a 55 34 5a 44 56 6a 4d 32 45 32 5a 44 67 35 59 7a 67 79 4e 7a 41 34 5a 6a 49 79 4f 57 51 7a 4e 7a 67 78 4e 6d 45 77 59 6a 42 68 5a 44 46 6a 4e 7a 41 77 4d 54 6b 35 4e 57 4e 6c 4f 54 5a 69 5a 44 70 37 49 6d 4e 76 64 57 35 30 63 6e 6b 69 4f 69 4a 56 55 79 49 73 49 6d 56 6b 61 58 52 70 62 32 34 69 4f 69 4a 7a 64 47 51 74 4d 53 49 73 49 6d 6c 75 63 33 52 68 62 47 78 6c 63 6c 39 75 59 57 31 6c 49 6a 6f 69 54 33 42 6c 63 6d 46 48 57 46 4e 6c 64 48 56 77 4c 6d 56 34 5a 53 49 73 49 6e 42 79 62 32 52 32 59 33 51 69 4f 69	[0329/191858.971:INFO:installer_main.cc(610)] Tracking data: ZWZhODRkMDMxNWM0NDNlYjU4ZDVjM2E2ZDg5YzgyNzA4ZjIyOWQzNzgxNmEwYjBhZDFjNzAwMTk5NWNlOTZiZDp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOi	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3273	88	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 73 65 74 74 69 6e 67 73 5f 69 6d 70 6c 2e 63 63 28 37 38 35 29 5d 20 46 6f 75 6e 64 20 33 20 70 61 74 68 73 20 66 6f 72 20 73 74 61 6e 64 61 6c 6f 6e 65 20 69 6e 73 74 61 6c 6c 20 6d 6f 64 65 2e 0a	[0329/191858.971:INFO:settings_impl.cc(785)] Found 3 paths for standalone install mode.	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3361	100	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 72 65 73 6f 75 72 63 65 5f 6c 31 30 6e 5f 68 61 6e 64 6c 65 72 2e 63 63 28 31 31 33 29 5d 20 4c 61 6e 67 75 61 67 65 20 6e 6f 74 20 69 6e 20 74 68 65 20 61 76 61 69 6c 61 62 6c 65 20 6c 61 6e 67 75 61 67 65 73 20 6c 69 73 74 3a 20 0a	[0329/191858.971:INFO:resource_l10n_handler.cc(113)] Language not in the available languages list:	success or wait	1	6AC5D6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3461	103	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 72 65 73 6f 75 72 63 65 5f 6c 31 30 6e 5f 68 61 6e 64 6c 65 72 2e 63 63 28 31 31 39 29 5d 20 54 72 79 69 6e 67 20 6c 61 6e 67 75 61 67 65 20 66 72 6f 6d 20 73 79 73 74 65 6d 20 70 72 65 66 65 72 72 65 64 20 6c 69 73 74 3a 20 65 6e 2d 47 42 0a	[0329/191858.971:INFO:resource_l10n_handler.cc(119)] Trying language from system preferred list: en-GB	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3564	114	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 73 65 74 74 69 6e 67 73 5f 69 6d 70 6c 2e 63 63 28 31 33 32 37 29 5d 20 49 6e 73 74 61 6c 6c 20 66 6f 6c 64 65 72 20 73 65 74 3a 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 50 72 6f 67 72 61 6d 73 5c 4f 70 65 72 61 20 47 58 0a	[0329/191858.971:INFO:settings_impl.cc(1327)] Install folder set: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3678	59	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 73 65 74 74 69 6e 67 73 5f 69 6d 70 6c 2e 63 63 28 31 33 38 32 29 5d 20 4f 70 65 72 61 74 69 6f 6e 3a 20 31 0a	[0329/191858.971:INFO:settings_impl.cc(1382)] Operation: 1	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3737	64	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 2e 63 63 28 31 39 36 29 5d 20 42 65 67 69 6e 6e 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 0a	[0329/191858.971:INFO:installer.cc(196)] Beginning installation	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3801	94	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 70 65 72 6d 69 73 73 69 6f 6e 5f 67 72 61 6e 74 6f 72 5f 69 6d 70 6c 2e 63 63 28 31 33 34 29 5d 20 57 72 69 74 65 20 70 72 69 76 69 6c 65 67 65 73 20 66 6f 72 20 69 6e 73 74 61 6c 6c 20 66 6f 6c 64 65 72 3a 20 31 0a	[0329/191858.971:INFO:permission_grantor_impl.cc(134)] Write privileges for install folder: 1	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3895	88	5b 30 33 32 39 2f 31 39 31 38 35 38 2e 39 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 5f 70 61 63 6b 61 67 65 5f 69 6d 70 6c 2e 63 63 28 37 30 29 5d 20 4e 65 65 64 20 74 6f 20 77 61 69 74 20 66 6f 72 20 61 63 74 75 61 6c 20 70 61 63 6b 61 67 65 0a	[0329/191858.971:INFO:installation_package_impl.cc(70)] Need to wait for actual package	success or wait	1	6AC5D6C3	WriteFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	32	32	20 00 00 00 13 00 00 00 3a 49 6e 73 74 61 6c 6c 65 72 20 6d 65 73 73 61 67 65 3a 00 09 00 00 00	:Installer message:	success or wait	171	6AB797B8	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	3983	74	5b 30 33 32 39 2f 31 39 31 39 32 34 2e 39 38 37 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 5f 70 61 63 6b 61 67 65 5f 69 6d 70 6c 2e 63 63 28 31 37 32 29 5d 20 50 61 63 6b 61 67 65 20 69 73 20 72 65 61 64 79 0a	[0329/191924.987:INFO:installation_package_impl.cc(172)] Package is ready	success or wait	1	6AC5D6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	4057	1835	5b 30 33 32 39 2f 31 39 31 39 35 34 2e 37 35 33 3a 49 4e 46 4f 3a 62 61 63 6b 65 6e 64 5f 70 72 6f 63 65 73 73 5f 6c 61 75 6e 63 68 65 72 5f 69 6d 70 6c 2e 63 63 28 31 32 31 29 5d 20 52 75 6e 6e 69 6e 67 20 69 6e 73 74 61 6c 6c 65 72 20 66 72 6f 6d 20 74 68 65 20 70 61 63 6b 61 67 65 20 77 69 74 68 20 63 6f 6d 6d 61 6e 64 20 6c 69 6e 65 3a 20 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 50 72 6f 67 72 61 6d 73 5c 4f 70 65 72 61 20 47 58 5c 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 5c 69 6e 73 74 61 6c 6c 65 72 2e 65 78 65 22 20 2d 2d 62 61 63 6b 65 6e 64 20 2d 2d 69 6e 69 74 69 61 6c 2d 70 69 64 3d 31 33 39 36 20 2d 2d 69 6e 73 74 61 6c 6c 20 2d 2d 69 6d 70 6f 72 74 2d 62 72 6f 77 73 65 72 2d 64 61 74 61 3d 30	[0329/191954.753:INFO:backend_process_launcher_impl.cc(121)] Running installer from the package with command line: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe" --backend --initial-pid=1396 --install --import-browser-data=0	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	5892	64	5b 30 33 32 39 2f 31 39 32 30 32 34 2e 30 39 34 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 2e 63 63 28 38 35 30 29 5d 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 73 75 63 63 65 65 64 65 64 0a	[0329/192024.094:INFO:installer.cc(850)] Installation succeeded	success or wait	1	6AC5D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	5956	95	5b 30 33 32 39 2f 31 39 32 30 32 34 2e 30 39 34 3a 49 4e 46 4f 3a 62 61 63 6b 65 6e 64 5f 70 72 6f 63 65 73 73 5f 69 6e 73 74 61 6c 6c 65 72 5f 72 75 6e 6e 65 72 5f 69 6d 70 6c 2e 63 63 28 31 38 37 29 5d 20 49 6e 73 74 61 6c 6c 65 72 20 62 61 63 6b 65 6e 64 20 65 78 69 74 69 6e 67 0a	[0329/192024.094:INFO:backend_process_installer_runner_impl.cc(187)] Installer backend exiting	success or wait	1	6AC5D6C3	WriteFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	11528	32	1c 00 00 00 13 00 00 00 3a 49 6e 73 74 61 6c 6c 65 72 20 6d 65 73 73 61 67 65 3a 00 01 00 00 00	:Installer message:	file forced closed	2	6AB797B8	WriteFile
unknown	unknown	106			invalid handle	2	6AD62B21	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191858956.log	6051	105	5b 30 33 32 39 2f 31 39 32 30 32 34 2e 30 39 34 3a 45 52 52 4f 52 3a 69 70 63 5f 73 65 6e 64 65 72 2e 63 63 28 31 31 33 29 5d 20 43 61 6e 6e 6f 74 20 77 72 69 74 65 20 74 6f 20 6d 61 69 6c 73 6c 6f 74 3a 20 52 65 61 63 68 65 64 20 74 68 65 20 65 6e 64 20 6f 66 20 74 68 65 20 66 69 6c 65 2e 20 28 30 78 32 36 29 0a	[0329/192024.094:ERROR:ipc_sender.cc(113)] Cannot write to mailslot: Reached the end of the file. (0x26)	success or wait	2	6AC5D6C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	6ACB5259	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	6ACB5259	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_20240329191858581\opera_package	0	1024	success or wait	92	6ACE6FFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\opera_package	0	3428	success or wait	1	6ACE70FC	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\opera_package	0	16384	success or wait	8647	6ACE70FC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Opera Software	success or wait	1	6AC22680	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Opera Software	Last Opera GX Stable Install Path	unicode	C:\Users\user\AppData\Local\Programs\Opera GX\	success or wait	1	6AD9E859	RegSetValueExW

Analysis Process: OperaGXSetup.exe PID: 4612, Parent PID: 652

General

Target ID:	7
Start time:	19:18:58
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\is-NM93K.tmp\OperaGXSetup.exe --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win32 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x308,0x30c,0x310,0x2d8,0x314,0x6aeb623c,0x6aeb6248,0x6aeb6254
Imagebase:	0x130000
File size:	3'581'600 bytes
MD5 hash:	3C5239C753641E08EA3C2080FBFD5D51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818588244612.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	132E97	CreateFileW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A74E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A74E67B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\attachments	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A74E67B	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818588244612.dll	success or wait	1	131979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291818588244612.dll	0	5449120	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 0a 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 33 00 00 38 1f 00 00 00 00 00 fd 26 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 54 00 00 04 00 00 fd fd 53 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 72 fd 3b 00 6d 00 00 00 e0 3b 00 fd 01 00	MZx@x!L!This program cannot be run in DOS mode.$PELf"!38&TS@Ar;m;	success or wait	1	132F54	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\crashpad_652_NAVCPLALIASLSMOQ	0	36	success or wait	2	6A765259	ReadFile
\pipe\crashpad_652_NAVCPLALIASLSMOQ	0	36	success or wait	1	6A765259	ReadFile

Analysis Process: Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe PID: **4952**, Parent PID: **1396**

General

Target ID:	9
Start time:	19:19:19
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe"
Imagebase:	0x400000
File size:	1'499'104 bytes
MD5 hash:	E9A2209B61F4BE34F25069A6E54AFFEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	401BAE	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40BF44	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\browser_assistant.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40BF44	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\files_list	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40BF44	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\mojo_core.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40BF44	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe	0	65536	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 09 00 fd 42 15 60 00 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 0e 00 00 60 16 00 00 fd 05 00 00 00 00 00 fd fd 13 00 00 10 00 00 00 00 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 1c 00 00 04 00 00 73 53 1c 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 1f fd 1a 00 60 00 00 00 7f fd 1a 00 18 01 00	MZx@x!L!This program cannot be run in DOS mode.$PELB`"`@sS@`	success or wait	26	40C086	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe	458752	65536	24 30 fd fd fd fd 3d 00 00 00 20 0f fd fd 02 00 00 29 49 fd fd fd 03 fd fd 02 39 fd 0f 42 01 fd fd fd fd 0f fd fd fd fd 1f 0f 42 fd 47 0c fd 44 24 2c 00 00 00 00 fd 44 24 30 fd fd 74 31 fd fd 00 00 00 20 0f fd 72 02 00 00 fd 04 fd 00 00 00 00 50 07 0c 00 fd fd 04 fd 15 fd 0f 7e 06 66 0f fd 02 fd 42 08 fd 47 04 fd 2a 02 00 00 31 fd fd 4d 0c 29 fd fd fd 03 fd 44 24 20 fd 0c 09 4c 24 28 fd 4c 24 24 fd 04 fd fd 44 24 2c fd 4c 24 20 fd 75 10 fd 32 02 00 00 fd 5c 24 24 fd 07 fd 4d 0c 29 fd fd fd 29 89 54 24 24 fd fd 7e 0b 51 50 52 fd fd 0c 00 fd fd 0c fd 47 04 fd 8b 4d 0c 29 85 fd 7e 1b 56 51 fd 74 24 30 fd fd 0c 00 fd fd 0c 03 74 24 28 fd 74 24 28 fd 47 04 fd 04 fd 74 24 28 fd 0f fd 54 24 24 fd 17 fd 4c 24 24 fd 77 04 fd 44 24	$0=)9BBGD$,D$0t1 rP~fBG*1M)D$ L$(L$$D$,L$ u2\$$M))T$$~QPRGM)~VQt$0t$(t$(Gt$(T$$L$$ wD$	success or wait	1	40C086	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe	589824	65536	fd fd 0a 73 0a fd 44 24 28 00 00 00 00 fd 18 fd 44 24 28 00 00 00 00 fd fd fd fd fd 06 72 06 04 fd 3c 06 73 76 fd 44 24 08 fd 0f 7e 40 10 0f fd 40 20 fd fd 24 fd 00 00 00 fd 11 0f fd fd fd 44 24 08 fd fd 24 fd 00 00 00 66 0f 7f 44 24 30 fd fd 24 fd 00 00 00 fd 08 fd fd 30 75 71 fd 4b 54 24 08 fd fd 24 fd 00 00 00 50 6a 10 fd 06 00 00 66 0f 6f 44 24 38 fd fd 08 fd fd 74 fd 66 0f fd fd fd 7c 24 18 00 0f fd 39 04 00 00 fd 0f 7e 05 10 fd 56 00 fd 2c 04 00 00 fd 44 24 08 fd 0f 10 40 10 66 0f fd 44 24 50 fd 44 24 50 fd 7c 24 08 fd fd 24 fd 03 00 00 31 fd fd fd 0a 00 fd 6c 24 08 fd 65 fd 5e 5f 5b 5d fd 10 00 fd 7d 10 00 fd 35 00 00 00 fd 18 00 00 00 0f 45 fd 74 24 2c 31 fd 31 fd fd 04 24 00 00 00 00 fd 44 24 20 00 00 00 00 0f fd 4d 5a 03	sD$(D$(r<svD$~@@ $D$$fD$0$0uqT $$PjfoD$8tf|$9~V,D$@fD PDP|$$ 1l$e^_[]}5Et$,11D Z	success or wait	1	40C086	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe	720896	65536	31 fd fd fd 06 fd fd 01 fd fd fd 09 fd 8b 7c 24 0c 31 fd fd 44 24 08 31 fd fd fd 0b 21 4d fd 13 4f 9c 5b 31 fd 31 fd fd 74 24 40 fd fd 02 01 fd 03 54 24 14 01 4b 4c 24 34 fd fd fd fd 0b fd fd fd fd 02 31 fd fd fd 03 fd fd 07 31 fd 31 fd fd fd 11 03 5c 24 3c fd fd 0a 03 5c 24 20 fd fd 31 cb 4c 24 18 fd fd 0e 01 fd fd 7c 24 1c 31 fd 5c 24 3c 31 fd fd fd 05 21 fd 74 24 14 31 fd 03 1c 24 31 fd fd fd 06 fd fd 01 fd fd fd 09 fd fd 7c 24 08 31 fd 6c 24 04 31 fd fd fd 0b 21 54 13 fd 6f 2e 68 31 fd 31 fd fd 4c 24 44 fd fd 02 01 fd 03 54 24 10 01 fd fd 74 24 38 fd fd fd fd 0b fd fd fd fd 02 31 fd fd fd 03 fd fd 07 31 fd 31 fd fd fd 11 03 5c 24 40 fd fd 0a 03 5c 24 24 fd fd 31 fd fd 74 24 14 fd fd 0e 01 fd fd 7c 24 18 31 89 5c 24	1|$1D$1!O[11t$@T$L$41 11\$<\$ 1 L$|$1\$<1!t$1$1|$1|$1!o. h11L$D T$t$8111\$@\$$1t$|$1\$	success or wait	1	40C086	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\browser_assistant.exe	0	46952	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 0a 00 fd 42 15 60 00 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 0e 00 00 08 27 00 00 0c 0b 00 00 00 00 00 fd 36 24 00 00 10 00 00 00 00 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 32 00 00 04 00 00 fd 76 32 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 dd 2f 00 5e 00 00 00 31 fd 2f 00 54 01 00	MZx@x!L!This program cannot be run in DOS mode.$PELB`'"6$@2v 2@/^1/T	success or wait	48	40C086	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\browser_assistant.exe	243560	65536	2a 6f 00 31 45 fd fd 0e 00 07 fd 0f 45 fd 5e 5f 5b 5d fd 0c 00 55 fd fd fd 15 29 6f 00 0f fd 01 fd 00 00 07 fd fd fd 0f 4f fd 5d fd 55 fd fd 53 57 56 fd fd fd 01 fd fd 67 00 fd 59 10 53 fd 15 20 fd 6f 00 fd 77 04 fd fd fd 00 00 00 53 fd 15 2a 6f 00 fd 7f 28 00 74 0b fd 47 28 00 53 fd 15 04 fd 6f 00 fd fd fd 79 00 00 00 fd fd 5e 5f 5b 5d fd fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 31 fd 40 5d fd 04 00 fd fd fd fd fd fd 55 fd fd 57 56 fd 75 08 fd 7e 10 57 fd 15 20 fd 6f 00 fd fd 04 fd fd fd 36 00 00 00 fd fd 57 fd 15 2a 6f 00 fd fd 5e 5f 5d fd 04 00 fd fd fd 55 fd fd 56 fd fd fd 5d fd fd fd fd 7d 08 00 74 09 56 fd 77 53 20 00 fd fd 04 fd fd 5e 5d fd 04 00 fd 55 fd fd 57 56 fd 8b 41 08 fd fd 7e 36 31 fd fd 0e fd 0c fd	o1E^_[]UoO]USWVgYS owSo(tG(Soy ^_[]U1@]UWVu~W o6Wo^_]UV]}tVwS ^]UWVA~61	success or wait	3	40C086	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\browser_assistant.exe	2471784	65536	08 fd 01 75 0a fd 45 08 fd 40 18 00 02 00 00 fd 45 08 fd 40 10 fd 56 57 53 50 fd 0d fd fd 23 83 fd 10 fd fd fd 75 04 0b fd fd 02 33 fd 5f 5e 5b 5d fd 6a 0c 68 68 fd 6f 00 fd fd 67 fd fd fd 7d 08 00 75 15 fd fd 6a fd fd fd 00 16 00 00 00 07 fd fd fd fd fd fd 47 fd 75 14 fd fd 74 0a fd fd 01 74 05 fd fd 02 75 83 4d fd fd fd 75 08 e9 fd fd 59 fd 65 fd 00 56 fd 75 10 fd 75 0c fd 75 08 fd fd fd fd fd fd fd 10 fd fd fd 75 fd fd 45 fd fd fd fd fd fd 15 00 00 00 fd 8b 4d fd 64 fd 0d 00 00 00 00 59 5f 5e 5b fd cb 75 fd fd 75 08 a9 fd fd 59 cb fd 55 fd fd 5d fd 05 00 00 fd fd 55 fd fd 5d fd fd 03 00 00 fd fd 55 fd fd 45 10 53 56 57 3c 01 74 32 3c 02 74 2e fd 4d 08 33 fd fd 45 0c 33 fd 33 fd 2b fd 39 4d 0c 1b fd fd fd 23 fd	uE@E@VWSP#u3_^[]jhhog}ujGuttuMuYeVuuuuEMdY_^[uuYU]U]UESVW<t2<t.M3E33+9M#	success or wait	1	40C086	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\mojo_core.dll	0	32403	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 42 15 60 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 0c 00 00 46 02 00 00 00 00 00 fd fd 0a 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 fd 0f 00 00 04 00 00 06 fd 0f 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 14 3f 0e 00 74 00 00 00 fd 3f 0e 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PELB`"!F@A?t?	success or wait	14	40C086	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\mojo_core.dll	425619	65536	fd 2f 0d 10 fd 44 24 40 68 fd 0e 10 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 49 20 fd 01 5d fd 60 08 fd fd fd fd 55 fd fd 53 57 56 fd 79 74 00 74 71 fd 75 08 fd 56 28 fd fd fd 00 00 00 0f 1f fd 00 00 00 00 00 fd c3 fd 0f 0f fd fd fd 30 0d 10 fd 58 04 fd fd 04 fd fd fd fd 75 51 fd 00 00 00 fd 40 04 78 66 fd 40 02 20 30 fd 76 10 0f 1f 40 00 fd fd fd 0f 0f fd fd fd 30 0d 10 fd 58 01 fd fd 04 fd fd fd fd 75 fd 66 fd 00 30 78 29 fd 52 50 fd 71 74 86 00 00 fd fd 0c 5e 5f 5b 5d fd 04 00 fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 49 20 fd 01 5d fd 60 04 fd fd fd fd 55 fd fd 49 20 fd 01 5d fd 60 18 fd fd fd fd 55 fd fd 53 57 56 fd fd 0c fd cb 55 08 fd fd fd 0b 00 00 fd fd fd 0b 00 00 fd fd 74 27 fd 01 39 fd	/D$@hUI]`USWVyttquV(0Xu@xf@ 0v@0Xuf0x)RPqt^_[]UI ]`UI]`USWVUt'9	success or wait	1	40C086	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\mojo_core.dll	949907	40453	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	40C086	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	0	4096	success or wait	24	40BFBE	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	0	4096	success or wait	516	40BFBE	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	0	32	success or wait	1	40BFBE	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	0	226	success or wait	1	40BFBE	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	0	48774	success or wait	2	40BFBE	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	0	203996	success or wait	1	40BFBE	ReadFile

Analysis Process: assistant_installer.exe PID: **4320**, Parent PID: **1396**

General

Target ID:	10
Start time:	19:19:20
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe" --version
Imagebase:	0xc00000
File size:	1'853'592 bytes
MD5 hash:	4C8FBED0044DA34AD25F781C3D117A66
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CC5332	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CC5332	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\assistant_installer_20240329191920.log	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	C4BD0B	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	73 64 50 43 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 41 fd fd 6d 1a fd 4e fd 3c fd fd 47 48 fd fd	sdPC\AmN<GH	success or wait	1	CFA4FA	WriteFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	73 64 50 43 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 41 fd fd 6d 1a fd 4e fd 3c fd fd 47 48 fd fd	sdPC\AmN<GH	success or wait	1	CFA4FA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\assistant_installer_20240329191920.log	0	244	5b 30 33 32 39 2f 31 39 31 39 32 30 2e 38 39 39 3a 49 4e 46 4f 3a 61 73 73 69 73 74 61 6e 74 5f 69 6e 73 74 61 6c 6c 65 72 5f 6d 61 69 6e 2e 63 63 28 31 36 39 29 5d 20 52 75 6e 6e 69 6e 67 20 61 73 73 69 73 74 61 6e 74 20 69 6e 73 74 61 6c 6c 65 72 20 77 69 74 68 20 63 6f 6d 6d 61 6e 64 20 6c 69 6e 65 20 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 2e 6f 70 65 72 61 5c 4f 70 65 72 61 20 47 58 20 49 6e 73 74 61 6c 6c 65 72 20 54 65 6d 70 5c 6f 70 65 72 61 5f 70 61 63 6b 61 67 65 5f 32 30 32 34 30 33 32 39 31 39 31 38 35 38 31 5c 61 73 73 69 73 74 61 6e 74 5c 61 73 73 69 73 74 61 6e 74 5f 69 6e 73 74 61 6c 6c 65 72 2e 65 78 65 22 20 2d 2d 76 65 72 73 69 6f 6e 0a	[0329/191920.899:INFO:assistant_installer_main.cc(169)] Running assistant installer with command line "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe" --version	success or wait	1	C4C493	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	CFA559	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	CFA559	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	CFA559	ReadFile

Analysis Process: assistant_installer.exe PID: **2964**, Parent PID: **4320**

General

Target ID:	11
Start time:	19:19:20
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\assistant\assistant_installer.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win32 --annotation=prod=OperaDesktopGX --annotation=ver=73.0.3856.382 --initial-client-data=0x270,0x274,0x278,0x24c,0x27c,0xdb4f48,0xdb4f58,0xdb4f64
Imagebase:	0xc00000
File size:	1'853'592 bytes
MD5 hash:	4C8FBED0044DA34AD25F781C3D117A66
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CC5332	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CC5332	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	CFA559	ReadFile
\pipe\crashpad_4320_BRAQNGZPNYUKGUDX	0	36	success or wait	1	CFA559	ReadFile
\pipe\crashpad_4320_BRAQNGZPNYUKGUDX	0	36	success or wait	1	CFA559	ReadFile

Analysis Process: installer.exe PID: **3504**, Parent PID: **652**

General

Target ID:	13
Start time:	19:19:54
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe" --backend --initial-pid=1396 --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --consent-given=0 --general-interests=0 --general-location=0 --personalized-content=0 --personalized-ads=0 --launchopera=1 --installfolder="C:\Users\user\AppData\Local\Programs\Opera GX" --profile-folder --language=en-GB --singleprofile=0 --copyonly=0 --allusers=0 --setdefaultbrowser=1 --pintotaskbar=1 --pintostartmenu=1 --run-at-startup=1 --server-tracking-data=server_tracking_data --package-dir="C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581" --session-guid=8ddbc8bc-ca9a-4c2b-a001-468713504759 --server-tracking-blob=NGFjMjBjZGM2OTE2N2RiNmJlYjJmY2M2YTBmZDdmMDY4ZjE3N2Y3OWFjNmExN2RhOTU2NGUyNWUyOTFkYjhlNjp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4LWdlbmVyaWMiLCJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21IZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04MDVjOTQ2ZWM3YzU0NjgwYjM3ZjU4MmQ1OGRlMTgzMCZ1dG1fY29udGVudD0zNzQyX3NldHVwaW8iLCJzeXN0ZW0iOnsicGxhdGZvcm0iOnsiYXJjaCI6Ing4NI82NCIsIm9wc3lzIjoiV2luZG93cyIsIm9wc3lzLXZlcnNpb24iOiIxMCIsInBhY2thZ2UiOiJFWEUifX0sInRpbWVzdGFtcCI6IjE3MTE3MzYzMzYuNTM0NCIsInVzZXJhZ2VudCI6Iklubm8gU2V0dXAgNi4yLjIiLCJ1dG0iOnsiY2FtcGFpZ24iOiJQV05fVVNfUEI0XzM3NDIiLCJjb250ZW50Ijoi Mzc0Ml9zZXR1cGlvIiwiaWQiOiI4MDVjOTQ2ZWM3YzU0NjgwYjM3ZjU4MmQ1OGRlMTgzMCIsIm1IZGl1bSI6InBhIiwic291cmNlIjoiUFdOZ2FtZXMifSwidXVpZCI6ImFiN2E4MGUwLWY1MjItNDZjMy1iYzdlLWQxNzkzYjIwNDhlMiJ9 --silent --desktopshortcut=1 --install-subfolder=107.0.5045.79
Imagebase:	0x7ff65f4a0000
File size:	6'949'792 bytes
MD5 hash:	21AD4599ABD2E158DB5128F32D3CC4EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs • Detection: 0%, Virustotal, Browse
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291819548603504.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF65F4A2DB4	CreateFileW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8A8B2BC80	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\reports	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8A8B2BC80	CreateDirectoryW
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\attachments	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8A8B2BC80	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329191955376.log	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF8A8C68B18	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\Assets	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8A8AC93DF	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\server_tracking_data	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8A8AC9AE3	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\pref_default_overrides	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\Desktop\Opera GX Browser .lnk	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Opera GX Browser .lnk	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\installation_status.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8A8AC9AE3	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\done	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8A8AC9AE3	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\28443390-d0c3-48e2-a4b4-b93f535f981b.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8A8AC7E9E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe.1711736396.old	success or wait	1	7FF8A8AC8388	DeleteFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list.1711736395.old	success or wait	2	7FF8A8AC8388	DeleteFileW
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291819548603504.dll	success or wait	1	7FF65F4A1AD5	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list.1711736395.old	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list.1711736395.old	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-100.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-100.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-100_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-100_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-140.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-140.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-140_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-140_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-180.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-180.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-180_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-180_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-80.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-80.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\150x150Logo.scale-80_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\150x150Logo.scale-80_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-100.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-100.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-100_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-100_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-140.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-140.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-140_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-140_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-180.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-180.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-180_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-180_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-80.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-80.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Assets\70x70Logo.scale-80_contrast-white.png	C:\Users\user\AppData\Local\Programs\Opera GX\Assets\70x70Logo.scale-80_contrast-white.png	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\Resources.pri	C:\Users\user\AppData\Local\Programs\Opera GX\Resources.pri	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.visualelementsmanifest.xml	C:\Users\user\AppData\Local\Programs\Opera GX\launcher.visualelementsmanifest.xml	success or wait	1	7FF8A8C614E7	MoveFileExW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera.visualelementsmanifest.xml	C:\Users\user\AppData\Local\Programs\Opera GX\opera.visualelementsmanifest.xml	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe.1711736396.old	success or wait	1	7FF8A8C614E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\28443390-d0c3-48e2-a4b4-b93f535f981b.tmp	C:\Users\user\AppData\Local\Programs\Opera GX\installer_prefs.json	success or wait	1	7FF8A8AC860C	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291819548603504.dll	0	6319520	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 fd 0f 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 00 00 64 3e 00 00 fd 21 00 00 00 00 00 20 75 2e 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 62 00 00 04 00 00 fd 60 00 03 00 60 41 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEdf" d>! u.b``A	success or wait	1	7FF65F4A2C38	WriteFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	73 64 50 43 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 41 fd fd 6d 1a fd 4e fd 3c fd fd 47 48 fd fd	sdPC\AmN<GH	success or wait	1	7FF8A8B4941C	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	0	105	3c 61 73 73 65 6d 62 6c 79 0d 0a 20 20 78 6d 6c 6e 73 3d 27 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 31 27 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 27 31 2e 30 27 3e 0d 0a 20 20 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 0d 0a 20 20 20 20 20 20	<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'> <assemblyIdentity	success or wait	1	7FF8A8ADC10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	105	1780	6e 61 6d 65 3d 27 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 27 0d 0a 20 20 20 20 20 76 65 72 73 69 6f 6e 3d 27 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 27 0d 0a 20 20 20 20 20 74 79 70 65 3d 27 77 69 6e 33 32 27 2f 3e 0d 0a 20 20 3c 66 69 6c 65 20 6e 61 6d 65 3d 27 6f 70 65 72 61 5f 65 6c 66 2e 64 6c 6c 27 2f 3e 0d 0a 3c 2f 61 73 73 65 6d 62 6c 79 3e 0d 0a fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 fd 00 00 00 fd 08 06 00 00 00 3c 01 71 fd 00 00 08 4c 49 44 41 54 78 fd fd fd 31 01 00 00 00 fd 20 fd fd 36 fd 5e 60 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 7b 00 fd fd fd fd 00 fd 9f 6d f6 6d 5d f6 6d f6 6d f6 6d fe fc fd fd fd fd fd fd 5b 73 fd fd fd 93 fd 5f fd fd fd fd fd 4e fd 4e 77 12 fd fd 5f 77 fd	name='107.0.5045.79' version='107.0.5045.79' type='win32'/> <file name='opera_elf.dll'/> </assembly>PNGIHDR<q LIDATx1 6^`{mm]mmm[s_NNw_w	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	1885	128	4b fd a7 fd 40 6f fd 79 fd fd 2f 55 37 fd 63 fd fd 20 42 10 fd 33 fd fd fd 3f fd 03 fd fd 7a fd 2e fd 2d fd 25 6c 23 1f 5f fd 4f 6d fd 72 0f 4c fd 4b fd 19 fd 14 bf 45 53 fd fd fd 3b fd fd 16 fd 4f fd 4c 43 10 7f 39 7c 05 fd 55 28 28 7c 2a fd 19 7e fd 38 fd fd 03 3a fd fd 57 fd 74 13 7c 64 29 01 32 fd 19 fd 27 fd fd 2e fd 73 7f 1b 4e fd fd fd fd fd 74 fd 3f 53 4b fd fd	K@oy/U7c B3?z.-%l#OmrLKES;OLC9 |U((|*~8:Wt|d)2'.sNt?SK	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2013	58	1e fd fd 10 4f 00 fd 10 fd fd fd 35 1a fd c3 fd 3a fd 10 7e fd fd 04 2c 32 54 78 57 fd 09 1c 00 fd 6c fd fd 10 fd fd fd 50 fd 1b c6 fd 09 3e db 6e 3c 29 2e	O5:~,2TxWlPn<).	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2071	55	fd 3f fd 0b 5f 0a 2f fd 07 fd fd fd 04 fd fd fd fd 20 fd 7b 10 fd fd 68 fd 1e fd fd 7e fd 56 30 fd fd fd 4f fd 44 1d fd 02 5d fd 03 fd fd fd 5a fd 02 48 fd fd 30	?_/ {h~V0OD]ZH0	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2126	63	1c fd 41 3d 28 0f fd fd 03 fd fd fd 1c 47 fd fd fd fd 5a fd 29 fd 17 61 1d 58 fd 3c 07 3b 04 fd 65 fd fd 2c 4e fd 1c fd 21 fd fd 59 5c 31 50 07 fd 03 14 58 27 78 43 fd fd 6b 50 fd 56 33	A=(GZ)aX<;e,N!Y\1PX'xCkPV3	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2189	55	fd fd 1f fd fd 5e 4a fd 1b 15 fd 6c fd 02 58 03 fd fd 03 fd 10 5c 37 fd 02 fd fd 37 4c fd fd 78 05 fd 31 fd 7d fd 4b 0b fd 5b 73 fd 7d 00 fd 60 21 fd fd 12 fd 11 3e	^JIX\77Lx1}K[s}`!>	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2244	62	fd fd fd 19 78 16 87 1f fd 00 fd fd 49 70 fd fd 22 fd 20 fd fd 73 21 6d 17 fd fd 30 fd 4e fd 5e fd 07 19 6e fd fd fd 02 7b 08 4a fd 54 1e 06 70 68 0d 54 fd fd fd 28 6b fd fd 0e fd 40	xIp" s!m0N^n{JTphT(k@	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2306	59	0d 18 05 3b fd 5a 10 43 05 fd fd 7b fd fd 12 fd fd fd fd fd 4d fd 20 fd 1b fd fd fd fd a1 01 00 00 04 00 30 fd fd 6a fd 6e 69 73 5e 01 00 00 00 00 00 00 00 00 00 00	;ZC{M 0nis^	success or wait	1	7FF8A8ADC10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2365	88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4f 0b 50 fd 12 fd 29 fd 00 00 00 00 49 45 4e 44 fd 42 60 fd fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 fd 00 00 00 fd 08 04 00 00 00 fd 08 fd 69 00 00 06 fd 49 44 41 54 78 fd fd fd 69 fd	OPIENDB`PNGIHDRiIDATxi	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2453	100	5d 55 19 06 fd fd fd fd 16 fd 4a 0b 14 52 54 fd 48 11 fd 14 fd 54 1a fd fd 73 65 56 fd 18 29 62 fd 42 fd 35 fd 40 08 61 fd 51 11 10 50 10 63 fd 20 32 45 fd fd 1a fd 65 52 19 fd 18 50 28 fd fd 0d fd fd 50 fd fd fd fd fd fd fd 49 fd fd fd 73 fd 1f 76 ee fd fd 79 fd 7f fd 75 fd fd fd fd fd 51	]UJRTHTseV)bB5@aQPc 2EeRP(PIsvyuQ	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2553	103	14 45 51 14 45 51 14 45 51 14 45 51 14 45 51 14 45 51 14 45 51 14 45 51 14 45 51 0c fd 18 53 fd 6e fd fd fd 6a fd 15 22 b3 fd fd fd 70 fd fd 7c 42 fd fd 5d fd 09 fd fd 3e fd fd 9e fd fd fd fd 39 fd 33 32 fd fd fd 0a fd 59 fd 6c fd 52 1f fd 2a 79 fd 5c fd 38 fd 34 fd fd fd fd fd 70 fd 4b fd fd 45 59 25 7d fd	EQEQEQEQEQEQEQEQSnj"p|B]>932YlR*y\84pKEY%}	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2656	114	fd 35 fd 68 17 5b 2a fd 7c fd 56 fd fd 69 fd 46 fd fd 71 7e fd 0e fd 3b 06 fd 57 36 31 fd 4d 35 5f b9 fd 31 46 11 13 23 47 6a fd fd 49 5a fd fd 75 fd 20 fd 36 fd 2a fd 77 fd fd af fd 6f 53 fd fd 44 fd 72 fd 29 fd 55 fd fd 1c fd 6a 16 79 fd 23 1e fd 79 fd fd 55 fd 0c 3b 53 fd 2d 22 fd fd fd 6e fd fd 76 fd 5e 69 fd	5h[*|ViFq~;W61M5_1FGjlZu *woSDr)Ujy#yU;S-"nv^i	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2770	59	55 57 fd 6a 13 68 6b fd fd 1b 6e fb 33 fd d9 43 2c 11 11 fd 4c 52 65 5b fd 69 7f 7d fd fd fd fd 48 fd 7a 40 fd 39 f0 71 fd fd 22 fd 76 fd 55 39 07 22 22 6e fd	UWjhkn,LRe[i}Hz@9q"vU9""n	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2829	64	29 fd fd fd fd 44 44 fd 69 58 fd 62 fd fd fd fd fd 2a 27 fd fd fd fd 76 35 10 23 fd fd 7e fd 24 fd 37 fd 5d fd 2e 54 6d fd fd fd cc fd 69 fd fd fd 02 4e fd 2b fd fd fd 1a 6d fd fd 0a 78	)DDiXb*'v5#~$7].Tmi+mx	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2893	94	fd 6a 5f fd 27 22 4e 47 fd 5d fd fd 6e 07 6a fd 76 6c 7b fd fd 4c 73 fd fd fd 3b fd 54 71 3d 45 fd fd 33 fd fd fd 31 3b fd 76 fd fd 78 42 fd fd fd 2a 22 5e fd 31 55 fd fd 38 19 fd fd 78 4c 2c 37 5d fd fd fd 44 fd 39 1a 69 fd fd 22 fd fd 4e fd fd 22 fd fd fd 63 03 fd 44 fd	j_'"NG]njvl{Ls;T=E31;vxB*"^1U8xL,7]D9i"N"cD	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	2987	74	fd fd 58 fd 16 fd 63 2b 0d 74 fd fd 38 4d fd fd fd 5b fd 2e fd fd fd fd 22 66 fd fd fd fd fd fd fd fd fd 52 11 fd 30 52 fd 31 16 fd 58 68 fd fd 3b 4e 44 fd 3d 55 fd 49 44 fd 61 2e 15 11 fd fd 76 fd fd 38 fd fd fd 27 fd	Xc+t8M["fR0R1Xh;ND=UIDa.v8'	success or wait	1	7FF8A8ADC10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	0	262144	2f 2f 20 44 55 77 67 6b 7a 70 52 73 32 55 42 5a 44 51 49 37 37 2b 63 54 33 50 36 72 46 43 42 31 41 30 64 54 73 33 32 33 73 30 50 38 56 77 4b 50 4e 78 4a 67 37 55 43 37 36 51 44 62 63 43 52 4d 79 53 55 57 75 36 6f 53 31 79 7a 54 43 67 75 52 6c 55 59 54 63 69 64 71 70 65 5a 64 74 48 4f 4c 30 39 2f 7a 2b 6c 75 50 7a 49 48 48 71 42 2f 76 51 39 72 6e 6d 4b 76 4e 50 4a 70 47 72 42 4a 6b 4b 66 79 74 54 4f 75 77 39 76 38 66 72 44 65 5a 61 65 48 36 72 34 69 42 31 62 33 49 63 78 58 44 56 42 47 2f 63 5a 69 56 4d 76 68 6a 30 2f 62 39 53 62 41 62 6b 67 4e 39 34 47 55 72 44 6a 49 41 72 48 45 6f 34 39 65 42 4d 46 63 59 4b 75 4c 46 6a 4f 55 6d 62 69 52 75 45 53 46 6e 33 52 6c 78 31 53 46 4e 73 50 6b 32 47 45 6f 68 72 52 76 73 62 33 46 7a 68 39 55 48 36 68 77 4b 46 55 45	// DUwgkzpRs2UBZDQI77+cT3P6rFCB1A0dTs323s0P8VwKPNxJg7UC76QDbcCRMySUWu6oS1yzTCguRlUYTcidqpeZdtHOL09/z+luPzIHHqB/vQ9rnmKvNPJpGrBJkKfytTOuw9v8frDeZaeH6r4iB1b3IcxXDVBG/cZiVMvhj0/b9SbAbkgN94GUrDjIArHEo49eBMFcYKuLFjOUmbiRuESFn3Rlx1SFNsPk2GEohrRvsb3Fzh9UH6hwKFUE	success or wait	6	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3061	134	75 63 74 1a fd 03 11 0f 6b fd 71 3e 10 71 fd 6a 63 fd 2b 62 fd fd fd 46 fd fd fd fd 72 fd fd fd fd 41 4e 13 11 fd fd fd 7d 11 fd fd fd fd 59 fd 4a 13 6b 7e fd 3b 34 fd 33 22 1e 55 fd fd 05 11 73 0c fd 24 11 fd da fd 6e fd 71 1a 62 7b 11 71 fd 6a fd fd fd fd 0d 83 22 fd 59 5f fd fd 45 09 1a fd 62 11 3d fd 53 fd 22 fd 34 fd fd 1c 5b fd fd fd 53 fd 1c 0d fd 59 fd 36 4f fd 4c fd fd fd	uctkq>qjc+bFrAN}YJk~;43"Us$nqb{qj"Y_Eb=S"4[SY6OL	success or wait	2	7FF8A8ADC10D	WriteFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	32	32	20 00 00 00 13 00 00 00 3a 49 6e 73 74 61 6c 6c 65 72 20 6d 65 73 73 61 67 65 3a 00 09 00 00 00	:Installer message:	success or wait	76	7FF8A89CBFE1	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe	0	262144	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 fd 0b 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 00 00 fd 10 00 00 fd 05 00 00 00 00 00 10 25 0a 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 60 18 00 00 04 00 00 78 fd 17 00 02 00 60 fd 00 00 fd 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEdf"%@`x`	success or wait	6	7FF8A8A94F2E	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe	0	524288	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 fd 0d 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 00 00 2e 1b 00 00 fd 07 00 00 00 00 00 fd fd 12 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 24 00 00 04 00 00 78 2a 23 00 02 00 60 fd 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEdf".@$x*#`	success or wait	5	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\server_tracking_data	0	896	4e 47 46 6a 4d 6a 42 6a 5a 47 4d 32 4f 54 45 32 4e 32 52 69 4e 6d 4a 6c 59 6a 4a 6d 59 32 4d 32 59 54 42 6d 5a 44 64 6d 4d 44 59 34 5a 6a 45 33 4e 32 59 33 4f 57 46 6a 4e 6d 45 78 4e 32 52 68 4f 54 55 32 4e 47 55 79 4e 57 55 79 4f 54 46 6b 59 6a 68 6c 4e 6a 70 37 49 6d 4e 76 64 57 35 30 63 6e 6b 69 4f 69 4a 56 55 79 49 73 49 6d 56 6b 61 58 52 70 62 32 34 69 4f 69 4a 7a 64 47 51 74 4d 53 49 73 49 6d 6c 75 63 33 52 68 62 47 78 6c 63 6c 39 75 59 57 31 6c 49 6a 6f 69 54 33 42 6c 63 6d 46 48 57 46 4e 6c 64 48 56 77 4c 6d 56 34 5a 53 49 73 49 6e 42 79 62 32 52 31 59 33 51 69 4f 6e 73 69 62 6d 46 74 5a 53 49 36 49 6d 39 77 5a 58 4a 68 58 32 64 34 49 6e 30 73 49 6e 46 31 5a 58 4a 35 49 6a 6f 69 4c 32 39 77 5a 58 4a 68 58 32 64 34 4c 33 4e 30 59 57 4a 73 5a 53 39	NGFjMjBjZGM2OTE2N2RiNmJlYjJmY2M2YTBmZDdmMDY4ZjE3N2Y3OWFjNmExN2RhOTU2NGUyNWUyOTFkYjhlNjp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9	success or wait	1	7FF8A8AC9B47	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\pref_default_overrides	0	2	7b 7d	{}	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3334	71	21 fd 38 fd fd fd 45 44 fd fd 69 4c fd fd fd 56 fd 38 16 fd 22 62 0f 43 33 5b 44 6c fd fd 67 45 44 fd fd 5e fd fd 17 fd 2d fd fd fd 4e 44 4c fd 69 42 73 06 fd 4f 34 fd fd 60 6d 5c fd 7a 57 fd fd fd 6b fd	!8EDiLV8"bC3[DlgED^-NDLiBsO`mzWk	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3405	74	41 fd 9a fd 76 fd fd 2c fd fd fd 5f 13 71 fd fd 79 5a 44 fd 6e fd fd 68 fd 6a fd fd fd 1b 50 fd 51 11 67 1b fd fd 45 2c 50 65 fd fd 68 59 fd fd 22 fd 7e 54 fd fd fd 1b 0d fd 7a 22 fd 21 55 2e 13 fd 40 03 fd 27	Av_qyZDnhjPQgE,PehY"~Tz"!U.@'	success or wait	1	7FF8A8ADC10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Opera GX Browser .lnk	0	1435	4c 00 00 00 01 14 02 00 00 00 00 00 fd 00 00 00 00 00 00 46 fd 00 00 00 20 00 00 00 fd fd 7b fd 05 fd fd 01 fd fd 7b fd 05 fd fd 01 24 fd 3a fd 23 fd fd 01 fd 29 23 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 3a 00 1f 44 47 1a 03 59 72 3f fd 44 fd fd 55 fd fd 6b 30 fd 26 00 01 00 26 00 fd 10 00 00 00 20 4d c4 fd fd fd 01 58 fd 69 fd 05 fd fd 01 fd 02 fd fd 05 fd fd 01 14 00 fd 00 74 00 1c 00 43 46 53 46 16 00 31 00 00 00 00 00 44 57 53 6c 12 00 41 70 70 44 61 74 61 00 00 00 74 1a 59 5e fd fd fd 48 fd 67 17 33 fd fd 28 fd fd fd fd df 67 56 41 fd 47 fd fd 6b fd fd 7f 40 00 09 00 04 00 fd 44 57 53 6c 7d 58 57 fd 2e 00 00 00 42 fd 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 64 67 00 41 00 70 00 70 00 44	LF {{$:#)#(:DGYr? DUk0&& MXitCF SF1DWSlAppDatatY^Hg 3(gVAGk@DWS l}XW.BBdgAppD	success or wait	1	7FF8A8A94F2E	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Opera GX Browser .lnk	0	1435	4c 00 00 00 01 14 02 00 00 00 00 00 fd 00 00 00 00 00 00 46 fd 00 00 00 20 00 00 00 fd fd 7b fd 05 fd fd 01 fd fd 7b fd 05 fd fd 01 24 fd 3a fd 23 fd fd 01 fd 29 23 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 3a 00 1f 44 47 1a 03 59 72 3f fd 44 fd fd 55 fd fd 6b 30 fd 26 00 01 00 26 00 fd 10 00 00 00 20 4d c4 fd fd fd 01 58 fd 69 fd 05 fd fd 01 fd 02 fd fd 05 fd fd 01 14 00 fd 00 74 00 1c 00 43 46 53 46 16 00 31 00 00 00 00 00 44 57 53 6c 12 00 41 70 70 44 61 74 61 00 00 00 74 1a 59 5e fd fd fd 48 fd 67 17 33 fd fd 28 fd fd fd fd df 67 56 41 fd 47 fd fd 6b fd fd 7f 40 00 09 00 04 00 fd 44 57 53 6c 7d 58 57 fd 2e 00 00 00 42 fd 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 64 67 00 41 00 70 00 70 00 44	LF {{$:#)#(:DGYr? DUk0&& MXitCF SF1DWSlAppDatatY^Hg 3(gVAGk@DWS l}XW.BBdgAppD	success or wait	1	7FF8A8A94F2E	CopyFileW
unknown	unknown	61			invalid handle	1	7FF8A8C1560D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3479	60	62 fd fd fd 1f 37 14 5f 16 11 e9 32 4b fd 03 1a fd 1a 75 0a fd fd 58 fd 23 06 fd 14 fd fd fd 16 fd fd 52 03 fd fd fd fd 61 23 43 3f fd fd 25 22 26 b4 fd 47 69 fd 79 fd	b7_2KuX#Ra#C?%"&Giy	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3539	153	fd ca fd fd 60 fd fd 7d 11 eb 32 43 44 fd fd 08 3f 15 fd fd 5a fd 14 fd 67 0d fd 54 fd 19 fd 22 fd fd 21 fd fd 79 fd 09 5f 12 11 5f 30 38 fd fd fd 2d 75 fd fd 4f fd 79 1a 62 fd 37 44 fd 56 fd fd fd 44 fd fd 60 fd fd 23 62 6e fd 0b fd fd 68 fd fd 45 fd 62 fd 44 7a fd fd 0d fd 45 35 fd fd 51 fd fd fd 06 fd fd 4a 11 eb fd 0b 71 60 6f 51 29 3d 51 fd fd 46 fd 45 fd 72 fd fd 76 fd fd fd 26 19 fd fd 44 fd fd 5a fd fd fd 2a fd 35 fd 1a 65	`}2CD?ZgT"!y__08-uOyb7DVD`#bnh EDzE5QJqoQ=QFErv&DZ*5e	success or wait	1	7FF8A8ADC10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\installer_prefs_include.json.backup	0	1216	7b 22 63 6f 75 6e 74 72 79 22 3a 22 55 53 22 2c 22 66 65 61 74 75 72 65 73 2d 64 6e 61 2d 72 65 71 75 69 72 65 6d 65 6e 74 73 22 3a 7b 22 38 31 38 63 33 65 66 31 32 64 30 62 22 3a 7b 22 66 6f 72 62 69 64 64 65 6e 22 3a 5b 22 35 62 33 65 62 34 61 36 63 33 33 35 61 30 36 35 39 64 31 36 64 31 61 31 38 39 63 61 31 35 35 65 34 34 34 31 65 61 31 34 22 5d 2c 22 72 65 71 75 69 72 65 64 22 3a 5b 22 36 34 33 33 36 66 62 38 31 61 30 34 38 33 36 65 62 38 31 30 38 64 32 34 66 62 63 61 33 61 61 33 36 38 32 64 62 30 61 35 22 5d 7d 7d 2c 22 66 65 61 74 75 72 65 73 2d 72 65 6d 6f 74 65 2d 66 6c 61 67 22 3a 22 30 31 39 37 39 32 39 39 63 38 63 64 2c 31 33 65 30 32 35 66 36 34 62 64 36 3a 64 69 73 61 62 6c 65 64 2c 31 33 65 65 61 66 38 35 31 64 61 37 2c 31 35 33 32 32 66 34	{"country":"US","features-dna-requirements":{"818c3ef12d0b":{"forbidden":["5b3eb4a6c335a0659d16d1a189ca155e4441ea14"],"required":["64336fb81a04836eb8108d24fbca3aa3682db0a5"]}},"features-remote-flag":"01979299c8cd,13e025f64bd6:disabled,13eeaf851da7,15322f4	success or wait	1	7FF8A8C613BC	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3692	76	3b 11 71 fd 6a fd 7b 4b fd 23 fd fd fd 2e fd 44 fd fd fd 19 22 fd 3b 1a fd 46 11 71 00 fd 53 fd 12 fd fd fd fd 6b fd fd 4e fd fd 75 6b fd fd fd 17 fd 71 fd fd fd 23 22 fd fd 3f fd fd 12 71 fd fd 75 6a fd 5f 44 d1	;qj{K#.D";FqSkNukq#"?quj_D	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\installation_status.json	0	12876	7b 22 5f 61 6c 6c 5f 75 73 65 72 73 22 3a 66 61 6c 73 65 2c 22 5f 6c 61 75 6e 63 68 5f 66 72 6f 6d 5f 69 6e 73 74 61 6c 6c 5f 64 69 72 22 3a 74 72 75 65 2c 22 5f 73 6b 69 70 5f 6c 61 75 6e 63 68 65 72 22 3a 66 61 6c 73 65 2c 22 5f 73 75 62 66 6f 6c 64 65 72 22 3a 22 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 22 2c 22 61 70 70 5f 69 64 22 3a 22 31 37 31 31 37 33 36 33 39 35 22 2c 22 63 6f 70 79 5f 6f 6e 6c 79 22 3a 66 61 6c 73 65 2c 22 66 69 6c 65 73 22 3a 5b 22 31 30 37 2e 30 2e 35 30 34 35 2e 37 39 2e 6d 61 6e 69 66 65 73 74 22 2c 22 43 55 45 53 44 4b 2e 78 36 34 5f 32 30 31 37 2e 64 6c 6c 22 2c 22 4d 45 49 50 72 65 6c 6f 61 64 5c 5c 6d 61 6e 69 66 65 73 74 2e 6a 73 6f 6e 22 2c 22 4d 45 49 50 72 65 6c 6f 61 64 5c 5c 70 72 65 6c 6f 61 64 65 64 5f 64 61 74 61	{"_all_users":false,"_launch_from_install_dir":true,"_skip_launcher":false,"_subfolder":"107.0.5045.79","app_id":"1711736395","copy_only":false,"files":["107.0.5045.79.manifest","CUESDK.x64_2017.dll","MEIPreload\\manifest.json","MEIPreload\\preloaded_data	success or wait	1	7FF8A8AC9B47	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3768	71	fd fd 7e 2a 6e fd 75 11 1f fd 22 fd 5c 2b fd 6e 6b fd 72 fd fd fd 4d 43 fd fd 2b 22 fd 52 6d fd fd 22 fd 34 49 fd 2e 3f 13 4b fd fd fd be 7a 45 fd fd 06 1a fd fd fd 12 11 47 fd 76 fd fd 78 fd 64 54 1b 6b fd	~*nu"\+nkrMC+"Rm"4I.?KzEGvxdTk	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\done	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8A8AC9B47	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3839	76	6e fd fd 6a fd 7a 4f 44 fd fd 34 fd 3e 7a 45 2c 77 fd fd 2b fd 4b 7c 4b fd 11 fd fd fd 50 6d fd fd 0e fd 7f fd 4d 17 11 fd 1d fd fd fd 69 fd 6c 5d 03 fd 39 0b 45 fd 4c 4d 53 fd 5f fd 35 43 fd 6f fd 11 11 0b 4d fd fd 3f fd	jzOD4>zE,w+K|KPmMil]9ELMS_5CoM?	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	3915	156	fd fd 7e 6e fd 6e fd 05 22 22 6e fd fd 2a 3b 7b 4d 44 fd e6 19 fd fd 06 fd 68 fd f8 fd 28 fd fd 0c 7d 22 62 fd 29 fd fd 75 fd fd fd fd fd 0e fd 51 fd 36 74 fd 3b 2d fd 76 66 fd 32 fd 7c fd 62 11 fd fd 5a fd 54 fd fd fd 44 3b 56 7a ad fd 70 fd 19 fd 71 fd fd fd 24 fd fd fd a5 2d 3c 25 22 fd 5d fd 1a fd 53 fd 01 fd 4a 3f fd 0c 5b 23 fd fd 47 7b fd 5c 6d 1b 55 fd 76 fd fd 45 7d 6e 34 fd 30 fd fd 39 fd 1d 4f 3a fd 4e 5a 3a 6d 68 3f 67 fd fd fd	~nn""n*;{MDh(}"b)uQ6t;-vf2|bZTD;Vzpq$-<%"]SJ?[#G{\mUvE}n409O:NZ:mh?g	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	4071	64	5b 24 56 fd fd fd fd fd fd 63 fd 4a 16 7b 15 fd 3b fd 64 5b fd 60 33 3b fd f1 2e 35 fd 3b fd 4a 5e 31 fd 08 6b fd 5d 62 47 06 fd fd 1d 6a fd 35 fd 46 4e fd 07 e4 1f 79 fd 19 36	[$VJ{;d[`3;.5;J^1k]Gj5FNy6	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\f8eff576-81d5-4419-a836-b36d6019d97c.tmp	4135	95	fd fd 5b fd 7e fd 74 fd 17 2c fd 68 0c 5e 31 fd 65 0e fd fd fd 43 4b fd 2e 7a 74 19 fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 28 fd fd 18 fd fd 01 56 fd fd 74 29 fd e5 00 00 00 00 49 45 4e 44	[~t,h^1eCK.t((((((((((((((Vt)IEND	success or wait	1	7FF8A8ADC10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\28443390-d0c3-48e2-a4b4-b93f535f981b.tmp	0	1672	7b 22 61 6c 6c 2d 69 6e 73 74 61 6c 6c 65 72 2d 65 78 70 65 72 69 6d 65 6e 74 73 22 3a 5b 22 69 6e 73 74 61 6c 6c 65 72 2d 65 78 70 65 72 69 6d 65 6e 74 2d 74 65 73 74 40 32 22 2c 22 69 6e 73 74 61 6c 6c 65 72 2d 62 79 70 61 73 73 2d 6c 61 75 6e 63 68 65 72 40 32 22 5d 2c 22 61 75 74 6f 75 70 64 61 74 65 22 3a 66 61 6c 73 65 2c 22 62 72 6f 77 73 65 72 5f 65 64 69 74 69 6f 6e 22 3a 22 73 74 64 2d 31 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 55 53 22 2c 22 65 6e 61 62 6c 65 5f 73 74 61 74 73 22 3a 74 72 75 65 2c 22 66 65 61 74 75 72 65 73 2d 64 6e 61 2d 72 65 71 75 69 72 65 6d 65 6e 74 73 22 3a 7b 22 38 31 38 63 33 65 66 31 32 64 30 62 22 3a 7b 22 66 6f 72 62 69 64 64 65 6e 22 3a 5b 22 35 62 33 65 62 34 61 36 63 33 33 35 61 30 36 35 39 64 31 36 64 31 61 31 38	{"all-installer-experiments":["installer-experiment-test@2","installer-bypass-launcher@2"],"autoupdate":false,"browser_edition":"std-1","country":"US","enable_stats":true,"features-dna-requirements":{"818c3ef12d0b":{"forbidden":["5b3eb4a6c335a0659d16d1a18	success or wait	1	7FF8A8AC7587	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	7FF8A8B494B1	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	7FF8A8B494B1	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	0	4096	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	0	4096	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	0	4096	end of file	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list	0	4096	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list	0	4096	end of file	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\files_list	0	4096	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\files_list	0	4096	end of file	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\pref_default_overrides	0	4096	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\pref_default_overrides	0	4096	end of file	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\installer_prefs_include.json	0	4096	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291918581\installer_prefs_include.json	0	4096	end of file	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	0	1343488	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	0	4096	success or wait	1	7FF8A8C0F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	0	4096	end of file	1	7FF8A8C0F979	ReadFile

Analysis Process: installer.exe PID: **6188**, Parent PID: **3504**

General

Target ID:	14
Start time:	19:19:55
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x2c8,0x2cc,0x2d0,0x2a4,0x2d4,0x7ff8a8dad180,0x7ff8a8dad18c,0x7ff8a8dad198
Imagebase:	0x7ff65f4a0000
File size:	6'949'792 bytes
MD5 hash:	21AD4599ABD2E158DB5128F32D3CC4EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: explorer.exe PID: **1028**, Parent PID: **3504**

General

Target ID:	17
Start time:	19:20:02
Start date:	29/03/2024
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff674740000
File size:	5'141'208 bytes
MD5 hash:	662F4F92FDE3557E86D110526BB578D5
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

Analysis Process: launcher.exe PID: **5656**, Parent PID: **3504**

General	
Target ID:	18
Start time:	19:20:03
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe" --start-maximized
Imagebase:	0x7ff738410000
File size:	2'304'416 bytes
MD5 hash:	D737A64C835D918DBE53B2C7724488FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: launcher.exe PID: **1220**, Parent PID: **1068**

General	
Target ID:	19
Start time:	19:20:04
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe" --scheduledautoupdate 0
Imagebase:	0x7ff738410000
File size:	2'304'416 bytes
MD5 hash:	D737A64C835D918DBE53B2C7724488FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: opera_gx_splash.exe PID: **2992**, Parent PID: **5656**

General	
Target ID:	20
Start time:	19:20:05
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_gx_splash.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_gx_splash.exe" --instance-name=a7abe095bcfd6dc868442c2e858a30d1
Imagebase:	0x7ff7f8560000
File size:	2'231'200 bytes
MD5 hash:	706FE814240C22A6CB09FBF48CB86020
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: opera.exe PID: **3656**, Parent PID: **5656**

General	
Target ID:	21
Start time:	19:20:05
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --start-maximized --ran-launcher --instance-name=a7abe095bcfd6dc868442c2e858a30d1 --splash-handle=1040
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: opera_crashreporter.exe PID: **5860**, Parent PID: **3656**

General	
Target ID:	22
Start time:	19:20:06
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_crashreporter.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_crashreporter.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x284,0x288,0x28c,0x280,0x290,0x7ff8a6189628,0x7ff8a6189638,0x7ff8a6189648
Imagebase:	0x7ff6d5ad0000
File size:	2'019'744 bytes
MD5 hash:	26DF88B2E68E23B60C0EEAB3E29496BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: installer.exe PID: **2316**, Parent PID: **1220**

General	
Target ID:	23
Start time:	19:20:06
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\0EA40E5AB06B\installer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\0EA40E5AB06B\installer.exe" --version
Imagebase:	0x7ff69c7c0000
File size:	6'949'792 bytes
MD5 hash:	21AD4599ABD2E158DB5128F32D3CC4EE
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: opera.exe PID: **5144**, Parent PID: **1028**

General

Target ID:	24
Start time:	19:20:07
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --start-maximized --ran-launcher --instance-name=a7abe095bcfd6dc868442c2e858a30d1 --splash-handle=1040 --lowered-browser
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

Analysis Process: opera_crashreporter.exe PID: **2436**, Parent PID: **5144**

General

Target ID:	26
Start time:	19:20:08
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_crashreporter.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_crashreporter.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=OperaDesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x290,0x294,0x298,0x28c,0x29c,0x7ff8a6189628,0x7ff8a6189638,0x7ff8a6189648
Imagebase:	0x7ff6d5ad0000
File size:	2'019'744 bytes
MD5 hash:	26DF88B2E68E23B60C0EEAB3E29496BB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

Analysis Process: opera.exe PID: **2952**, Parent PID: **5144**

General

Target ID:	28
Start time:	19:20:09
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=gpu-process --no-appcompat-clear --start-stack-profiler --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAAACAAAAAAAAAAAIAAAAAAAAAAAA== --mojo-platform-channel-handle=1848 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:2
Imagebase:	0x7ff69a8b0000

File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

Analysis Process: opera_autoupdate.exe PID: **5516**, Parent PID: **1220**

General

Target ID:	29
Start time:	19:20:10
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe" --pipeid=oauc_task_piped42b87436846297e467003cba27fe2f4 --version=107.0.5045.79 --producttype --requesttype=automatic --downloaddir="C:\Users\user\AppData\Local\Temp\.opera\0EA40E5AB06B" --installationdatadir="C:\Users\user\AppData\Local\Programs\Opera GX" --operadir="C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79" --installdir="C:\Users\user\AppData\Local\Programs\Opera GX" --user-data-dir="C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable" --nometrics --scheduledtask
Imagebase:	0x7ff6e8050000
File size:	5'751'712 bytes
MD5 hash:	6026F4719045033EFD7EC6127ED6370C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs • Detection: 0%, Virustotal, Browse
Reputation:	low
Has exited:	true

Analysis Process: opera.exe PID: **5436**, Parent PID: **5144**

General

Target ID:	30
Start time:	19:20:10
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --enable-quic --no-appcompat-clear --start-stack-profiler --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=1972 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

Analysis Process: opera.exe PID: **3136**, Parent PID: **5144**

General

Target ID:	31
Start time:	19:20:10
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe

Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=2776 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

Analysis Process: opera.exe PID: **5372**, Parent PID: **5144**

General	
Target ID:	32
Start time:	19:20:11
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=3216 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: opera_autoupdate.exe PID: **2972**, Parent PID: **5516**

General	
Target ID:	33
Start time:	19:20:12
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_autoupdate.exe" --type=crashpad-handler "--user-data-dir=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports" "--crash-count-file=C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\crash_count.txt" --url=https://crashstats-collector.opera.com/collector/submit --annotation=channel=Stable --annotation=plat=Win64 --annotation=prod=Opera DesktopGX --annotation=ver=107.0.5045.79 --initial-client-data=0x22c,0x230,0x234,0x208,0x238,0x7ff6e85938fc,0x7ff6e8593908,0x7ff6e8593918
Imagebase:	0x7ff6e8050000
File size:	5'751'712 bytes
MD5 hash:	6026F4719045033EFD7EC6127ED6370C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: opera.exe PID: **3204**, Parent PID: **5144**

General	
Target ID:	35

Start time:	19:20:12
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=3356 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: koksDTqWjvmuJdFhyPGiECl.exe PID: **6416**, Parent PID: **3504**

General

Target ID:	36
Start time:	19:20:13
Start date:	29/03/2024
Path:	C:\Program Files (x86)\iVbaHhMGgjRPQdstHmqQTgkbxiYBLxBpyzsEuAKAsKqyZeBOViMTYbkOnfuIVKzSyxpCQrvLHujso\koksDTqWjvmuJdFhyPGiECl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\iVbaHhMGgjRPQdstHmqQTgkbxiYBLxBpyzsEuAKAsKqyZeBOViMTYbkOnfuIVKzSyxpCQrvLHujso\koksDTqWjvmuJdFhyPGiECl.exe"
Imagebase:	0x20000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

Analysis Process: opera.exe PID: **5336**, Parent PID: **5144**

General

Target ID:	37
Start time:	19:20:16
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=4364 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: koksDTqWjvmuJdFhyPGiECl.exe PID: **1096**, Parent PID: **3504**

General

Target ID:	38
Start time:	19:20:17
Start date:	29/03/2024
Path:	C:\Program Files (x86)\iVbaHhMGgjRPQdstHmqQTgkbxiYBLxBpyzsEuAKAsKqyZeBOViMTYbkOnfuIVKzSyxpCQrvLHujso\koksDTqWjvmuJdFhyPGiECl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\iVbaHhMGgjRPQdstHmqQTgkbxiYBLxBpyzsEuAKAsKqyZeBOViMTYbkOnfuIVKzSyxpCQrvLHujso\koksDTqWjvmuJdFhyPGiECl.exe"
Imagebase:	0x20000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

Analysis Process: opera.exe PID: **6452**, Parent PID: **5144**

General

Target ID:	39
Start time:	19:20:17
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-GB --service-sandbox-type=service --enable-quic --no-appcompat-clear --ab_tests=GXCTest50-test:DNA-99214_GXCTest50 --mojo-platform-channel-handle=4764 --field-trial-handle=1860,i,17205455559367761425,8087887266479412671,262144 --variations-seed-version /prefetch:8
Imagebase:	0x7ff69a8b0000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Disassembly

No disassembly