ID: 1417615
Sample Name:
SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe
Cookbook: default.jbs
Time: 19:34:13
Date: 29/03/2024
Version: 40.0.0 Tourmaline

Table of Contents

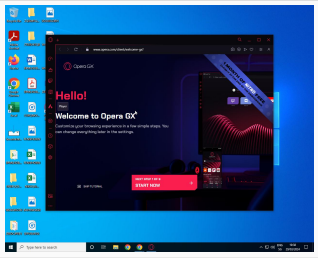
Windows Analysis Report

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:	38
Range:	0 - 100
Whitelisted:	false
Confidence:	0%

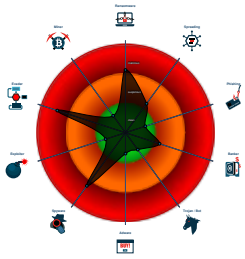
Compliance

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…
- Queries memory information (via WM…
- Queries sensitive physical memory …
- 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…

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: 6960 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe" MD5: DBB69EE00786BED3E12A04518E0F469A)
  - SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp (PID: 7004 cmdline: "C:\Users\user\AppData\Local\Temp\is-6G7J7.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp" /SL5="$2040C,1055917,832512,C:\Users\user\Desktop\SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe" MD5: 668D5368DEF8B65631C43EECBD50EA48)
    - OperaGXSetup.exe (PID: 5424 cmdline: "C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe" --silent --allusers=0 MD5: 1033B8A679409AAE694776CF2FDD3E8D)
      - OperaGXSetup.exe (PID: 5172 cmdline: C:\Users\user\AppData\Local\Temp\is-U02B5.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=0x2f4,0x2f8,0x2fc,0x2d0,0x300,0x6bc5623c,0x6bc56248,0x6bc56254 MD5: 1033B8A679409AAE694776CF2FDD3E8D)
      - OperaGXSetup.exe (PID: 5980 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\OperaGXSetup.exe" --version MD5: 1033B8A679409AAE694776CF2FDD3E8D)
      - OperaGXSetup.exe (PID: 3716 cmdline: "C:\Users\user\AppData\Local\Temp\is-U02B5.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=5424 --package-dir-prefix="C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_20240329193551" --session-guid=e8c1f83b-82a0-4cf5-8d29-c848e8638bca --server-tracking-blob=ZmUxNWFlNzQyYjk1NzA4ZTljODEyOGM4ZDY1NDg0M2YyNmVhN2MxNjg3MDQ5YmEyMGNjNzFjMzEyNjU5MGZjZTp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21lZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04NmE3YmY5NzI1Yjk0NDYxYjMzYzMzMGM3ZTA5NDUwMSZ1dG1fY29udGVudD0zNzQyX3NldHVwaW8iLCJzeXN0ZW0iOnsicGxhdGZvcm0iOnsiYXJjaCI6Ing4NI82NCIsIm9wc3lzIjoiV2l

uZG93cyIsIm9wc3lzLXZlcnNpb24iOiIxMCIsInBhY2thZ2UiOiJFWEUifX0sInRpbWVzdGFtcCI6IjE3MTE3MzczMjMuMDMxNCIsInVzZXJhZ2VudCI6Iklubm8gU2V0d XAgNi4yLjIiLCJ1dG0iOnsiY2FtcGFpZ24iOiJQV05fVVNfUEI0XzM3NDIiLCJjb250ZW50IjoiMzc0Ml9zZXR1cGlvIiwiaWQiOiI4NmE3YmY5NzI1Yjk0NDYxYjMzYzM zMGM3ZTA5NDUwMSIsIm1lZGl1bSI6InBhIiwic291cmNlIjoiUFdOZ2FtZXMifSwidXVpZCI6ImU1ZWJhZDA2LTcxY2MtNDg4Ny1hOGRmLTdlYTdjNzkwMzhhYSJ9 --silent --desktopshortcut=1 --wait-for-package --initial-proc-handle=9C05000000000000 MD5: 1033B8A679409AAE694776CF2FDD3E8D)

- OperaGXSetup.exe (PID: 2656 cmdline: C:\Users\user\AppData\Local\Temp\is-U02B5.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=0x300,0x304,0x308,0x2d0,0x30c,0x6afc623c,0x6afc6248,0x6afc6254 MD5: 1033B8A679409AAE694776CF2FDD3E8D)
- installer.exe (PID: 6324 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe" --backend --initial-pid=5424 --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_202403291935511" --session-guid=e8c1f83b-82a0-4cf5-8d29-c848e8638bca --server-tracking-blob=ZmUxNWFlNzQyYjk1NzA4ZTljODEyOGM4ZDY1NDg0M2YyNmVhN2MxNjg3MDQ5YmEyMGNjNzFjMzEyNjU5MGZjZTp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21lZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04NmE3YmY5NzI1Yjk0NDYxYjMzYzMzMGM3ZTA5NDUwMSZ1dG1fY29udGVudD0zNzQyX3NldHVwaW8iLCJzeXN0ZW0iOnsicGxhdGZvcm0iOnsiYXJjaCI6Ing4NI82NCIsIm9wc3lzIjoiV2luZG93cyIsIm9wc3lzLXZlcnNpb24iOiIxMCIsInBhY2thZ2UiOiJFWEUifX0sInRpbWVzdGFtcCI6IjE3MTE3MzczMjMuMDMxNCIsInVzZXJhZ2VudCI6Iklubm8gU2V0dXAgNi4yLjIiLCJ1dG0iOnsiY2FtcGFpZ24iOiJQV05fVVNfUEI0XzM3NDIiLCJjb250ZW50IjoiMzc0Ml9zZXR1cGlvIiwiaWQiOiI4NmE3YmY5NzI1Yjk0NDYxYjMzYzMzMGM3ZTA5NDUwMSIsIm1lZGl1bSI6InBhIiwic291cmNlIjoiUFdOZ2FtZXMifSwidXVpZCI6ImU1ZWJhZDA2LTcxY2MtNDg4Ny1hOGRmLTdlYTdjNzkwMzhhYSJ9 --silent --desktopshortcut=1 --install-subfolder=107.0.5045.79 MD5: 21AD4599ABD2E158DB5128F32D3CC4EE)
  - installer.exe (PID: 6936 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=0x2c0,0x2c4,0x2c8,0x29c,0x2cc,0x7ffdfb93d180,0x7ffdfb93d18c,0x7ffdfb93d198 MD5: 21AD4599ABD2E158DB5128F32D3CC4EE)
  - explorer.exe (PID: 2580 cmdline: C:\Windows\Explorer.EXE MD5: 662F4F92FDE3557E86D110526BB578D5)
    - opera.exe (PID: 6668 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --start-maximized --ran-launcher --instance-name=0e78e69c624cbcf87c7f299659eb65c0 --splash-handle=1040 --lowered-browser MD5: F452A15BC7E4392149F6BB2675EAAA59)
  - rrcsBizXUHISSeck.exe (PID: 1704 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 5668 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 2896 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 4020 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 1004 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 1456 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 4996 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 5300 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 5676 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 3808 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - launcher.exe (PID: 4900 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe" --start-maximized MD5: D737A64C835D918DBE53B2C7724488FF)
    - opera_gx_splash.exe (PID: 4820 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\opera_gx_splash.exe" --instance-name=0e78e69c624cbcf87c7f299659eb65c0 MD5: 706FE814240C22A6CB09FBF48CB86020)
    - opera.exe (PID: 5252 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\opera.exe" --start-maximized --ran-launcher --instance-name=0e78e69c624cbcf87c7f299659eb65c0 --splash-handle=1040 MD5: F452A15BC7E4392149F6BB2675EAAA59)
      - opera_crashreporter.exe (PID: 6412 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,0x280,0x290,0x7ffdf2ce9628,0x7ffdf2ce9638,0x7ffdf2ce9648 MD5: 26DF88B2E68E23B60C0EEAB3E29496BB)
  - rrcsBizXUHISSeck.exe (PID: 3004 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 2648 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 2852 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 6012 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
  - rrcsBizXUHISSeck.exe (PID: 3584 cmdline: "C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
- Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe (PID: 5184 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe" MD5: E9A2209B61F4BE34F25069A6E54AFFEA)
- assistant_installer.exe (PID: 2136 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\assistant_installer.exe" --version MD5: 4C8FBED0044DA34AD25F781C3D117A66)
  - assistant_installer.exe (PID: 3128 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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,0x494f48,0x494f58,0x494f64 MD5: 4C8FBED0044DA34AD25F781C3D117A66)

- launcher.exe (PID: 2932 cmdline: "C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe" --scheduledautoupdate 0 MD5: D737A64C835D918DBE53B2C7724488FF)
  - installer.exe (PID: 6692 cmdline: "C:\Users\user\AppData\Local\Temp\.opera\BDDCE5348F09\installer.exe" --version MD5: 21AD4599ABD2E158DB5128F32D3CC4EE)
- **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

Malware Analysis System Evasion

Queries memory information (via WMI often done to detect virtual machines)

Queries sensitive physical memory information (via WMI, Win32_PhysicalMemory, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Found direct / indirect Syscall (likely to bypass EDR)

Stealing of Sensitive Information

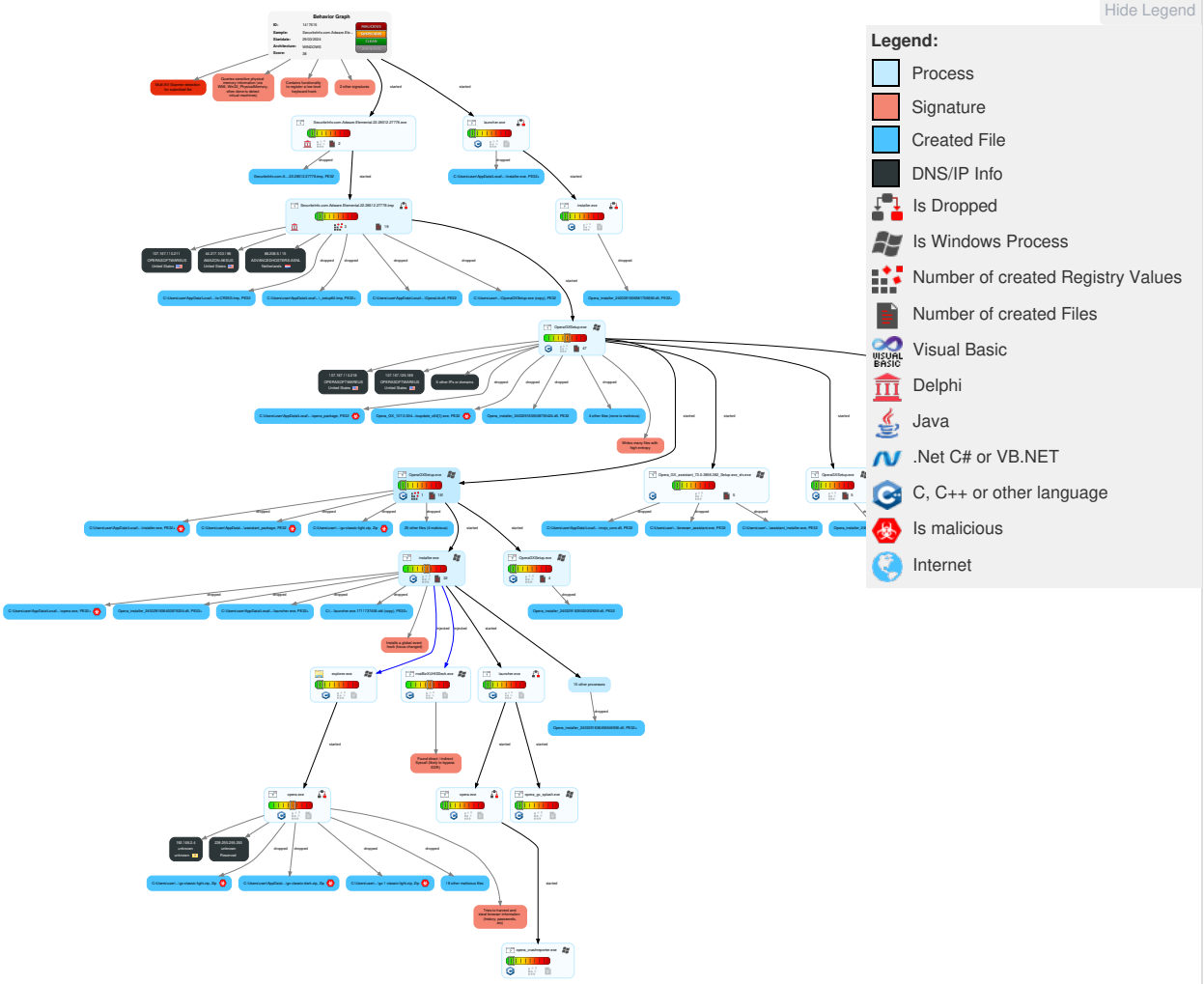
Tries to harvest and steal browser information (history, passwords, etc)

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	2 2 Windows Management Instrumentation	1 DLL Side-Loading	1 Abuse Elevation Control Mechanism	1 Disable or Modify Tools	1 OS Credential Dumping	1 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	1 Scheduled Task/Job	1 Windows Service	1 Valid Accounts	2 1 Obfuscated Files or Information	NTDS	7 6 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	1 Scheduled Task/Job	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	2 3 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	1 Scheduled Task/Job	1 DLL Search Order Hijacking	Proc Filesystem	1 3 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
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

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Org Information	DNS Server	Compromise Software Supply Chain	Windows Command Shell	Scheduled Task	Scheduled Task	1 3 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

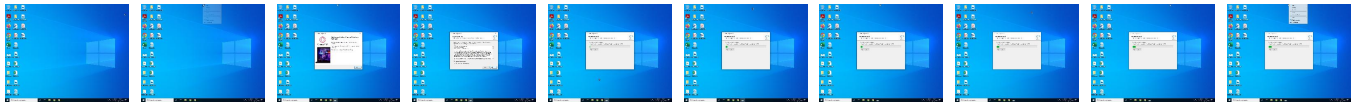
Behavior Graph

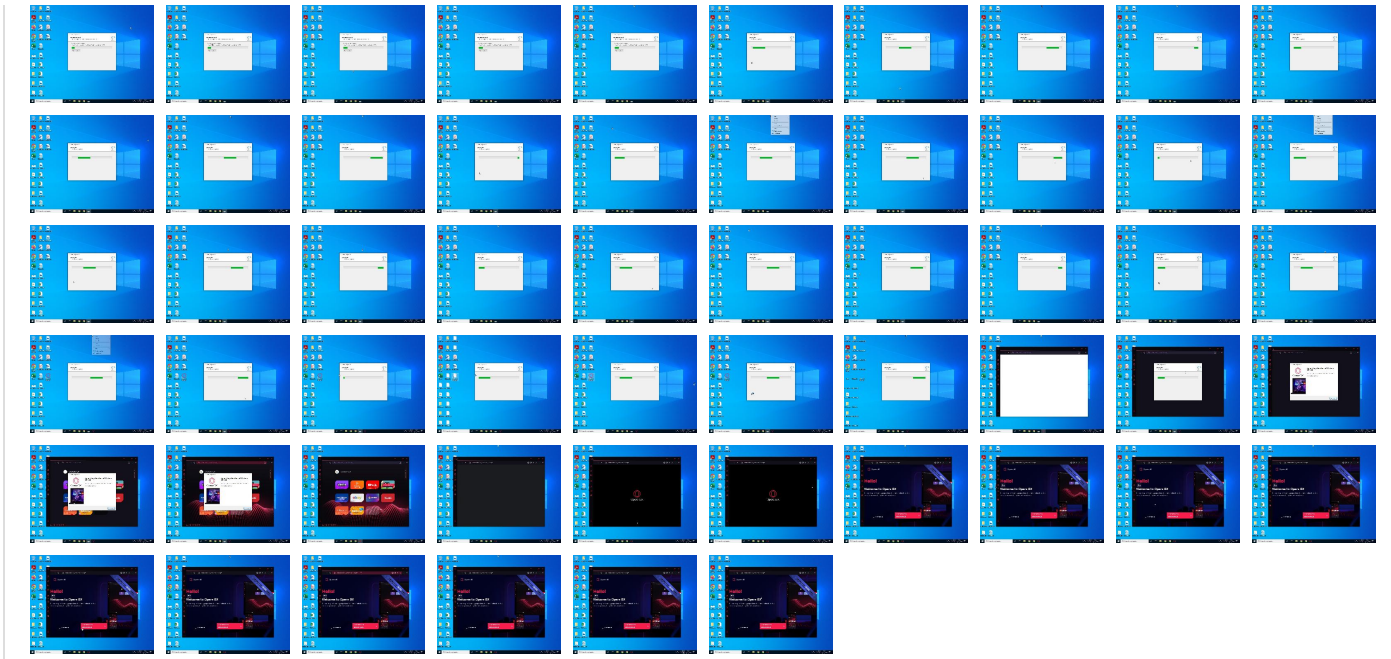


Screenshots

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	47%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\Opera_GX_assistant_73.0.3856.382_Setup[1].exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\Opera_GX_assistant_73.0.3856.382_Setup[1].exe	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZVZFKMB9\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.1711737406.old (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe.1711737406.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

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://autoupdate-staging.services.ams.osa/	0%	URL Reputation	safe	
http://autoupdate-staging.services.ams.osa/	0%	URL Reputation	safe	
http://https://simpleflying.com/how-do-you-become-an-air-traffic-controller/	0%	URL Reputation	safe	
http://https://www.remobjects.com/ps	0%	URL Reputation	safe	
http://autoupdate-staging.services.ams.osa/v4/v5/netinstaller///windows/x64v2/Fetching	0%	URL Reputation	safe	
http://https://outlook.com_	0%	URL Reputation	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/b	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://partners-offapi.net/apiBundle/geo?sourceID=31120&subId_1=361D4F6E-6488-4FB2-BF8B-32AC8683517	0%	Avira URL Cloud	safe	
http://localhost:3001api/prefs/?product=$1&version=$2..	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/U	0%	Avira URL Cloud	safe	
http://https://net.geo.opera.com8R7/KLRL579/	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryera.software	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryve7	0%	Avira URL Cloud	safe	
http://https://www.innosetup.com/	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryCx	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/b	0%	Virustotal		Browse
http://https://www.innosetup.com/	1%	Virustotal		Browse
http://https://yandex.com.tr/search/?clid=1669559&text=	0%	Avira URL Cloud	safe	
http://www.kymoto.orgA	0%	Avira URL Cloud	safe	
http://www.kymoto.orgAbout	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/6~	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/U	0%	Virustotal		Browse
http://https://yandex.com.tr/search/?clid=1669559&text=	0%	Virustotal		Browse
http://https://gamemaker.io)	0%	Avira URL Cloud	safe	
http://https://features.opera-api2.com/)l	0%	Avira URL Cloud	safe	
http://crl4.digg	0%	Avira URL Cloud	safe	
http://https://partners-offapi.net/apiBundle/stpstat	0%	Avira URL Cloud	safe	
http://https://gamemaker.io/en/get.	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryera.software	0%	Virustotal		Browse
http://https://desktop-netinstaller-sub.osp.opera.software/6~	0%	Virustotal		Browse
http://https://gamemaker.io	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binarytx	0%	Avira URL Cloud	safe	
http://https://partners-offapi.net/apiBundle/stpstat	1%	Virustotal		Browse
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryBy	0%	Avira URL Cloud	safe	
http://https://gamemaker.io/en/get.	0%	Virustotal		Browse
http://https://smolecular.icu/tfg/?src=setupIO	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/r-sub.osp.opera.software/	0%	Avira URL Cloud	safe	
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryBy	0%	Virustotal		Browse
http://https://gamemaker.io	0%	Virustotal		Browse
http://https://config.gx.games/	0%	Avira URL Cloud	safe	
http://https://smolecular.icu/tfg/?src=setupIO	0%	Virustotal		Browse
http://https://desktop-netinstaller-sub.osp.opera.software/r-sub.osp.opera.software/	0%	Virustotal		Browse
http://https://config.gx.games/	0%	Virustotal		Browse
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryCx	0%	Virustotal		Browse
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binarytx	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

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, 00000001.00000003.2983667346.0000000003CF1000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2985134000.0000000000870000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2968654031.0000000000876000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2977724410.0000000002398000.00000004.00001000.00020000.00000000.sdmp, explorer.exe, 00000012.00000000.2712316828.00000000018A0000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 00000013.00000000.2739420869.00000000012F0000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 00000014.00000000.2740429131.0000000001330000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 00000015.00000000.2741486699.0000000001500000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 00000016.00000000.2742508996.0000000001870000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 00000017.00000000.2743307763.00000000010E0000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 00000018.00000000.2744169384.0000000000EC0000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 00000019.00000000.2745906045.0000000001830000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 0000001A.00000000.2749446919.0000000001110000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 0000001B.00000000.2752926892.00000000016E0000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 0000001C.00000000.2754804739.0000000001670000.00000002.00000001.00040000.00000000.sdmp, rrcsBizXUHISSeck.exe, 0000001E.00000000.2778762112.0000000001AB1000.00000002.00000001.00040000.00000000.sdmp	false		high
http://https://aka.ms/odirmr	explorer.exe, 00000012.00000000.2713624554.00000000079FB000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://net.geo.opera.com8R7/KLRL579/	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2977724410.00000000242D000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://yandex.ua/search/?clid=2358536&text=	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://legal.opera.com/terms	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2964326998.0000000003E80000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2983667346.0000000003D0B000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2966678264.0000000003D11000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000002.2884160745.000000000105A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000006.00000002.2895156720.000000000105A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000007.00000002.2146216434.0000000000A3A000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000008.00000002.2872841518.000000000105A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000009.00000002.2880101734.000000000105A000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false		high
http://https://www.deezer.com/sr/login	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.browser.yandex.ua/suggest/get?part=	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13f2DV	explorer.exe, 00000012.00000000.2713624554.000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://download.opera.com/u	OperaGXSetup.exe, 00000005.00000003.2162819871.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2161348409.0000000001A65000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://help.opera.com/latest/	OperaGXSetup.exe, OperaGXSetup.exe, 00000009.00000002.2880101734.000000001080000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, launcher.exe, 0000001D.00000002.2813281163.000052F800288000.00000004.00001000.00020000.00000000.sdmp, opera.exe, 00000021.00000002.2818715184.000073F000254000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.msn.com:443/v1/news/Feed/Windows?	explorer.exe, 00000012.00000000.2715945417.00000000097D4000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000012.00000000.2713624554.000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://addons.opera.com/extensions/download/13655f413caacdcc677b24dc0c615d1f5328d6a3/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://download5.operacdn.com/lf	OperaGXSetup.exe, 00000005.00000002.2890469695.0000000004FF0000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://policies.google.com/terms;	OperaGXSetup.exe, 00000005.00000002.2884160745.000000000105A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000006.00000002.2895156720.0000000000105A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000007.00000002.2146216434.0000000000A3A000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000008.00000002.2872841518.000000000105A000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000009.00000002.2880101734.000000000105A000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false		high
http://https://www.baidu.com/favicon.ico	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://ff.search.yahoo.com/gossip?output=fxjson&command=	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://autoupdate-staging.services.ams.osa/	OperaGXSetup.exe	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://desktop-netinstaller-sub.osp.opera.software/b	OperaGXSetup.exe, 00000005.00000002.2887132236.0000000001A0B000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://localhost:3001api/prefs/?product=$1&version=$2..	OperaGXSetup.exe, 00000005.00000002.2884160745.0000000001080000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000006.00000002.2895156720.0000000001080000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000007.00000002.2146216434.0000000000A60000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000008.00000002.2872841518.0000000001080000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000009.00000002.2880101734.000000001080000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false	• Avira URL Cloud: safe	low
http://www.opera.com	OperaGXSetup.exe, 00000005.00000003.2350253023.000000004914C000.00000004.00001000.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2506614581.0000000049160000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://crashpad.chromium.org/https://crashpad.chromium.org/bug/new	OperaGXSetup.exe, 00000005.00000002.2884160745.0000000001080000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000006.00000002.2895156720.0000000001080000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000007.00000002.2146216434.0000000000A60000.00000040.00000001.01000000.0000000B.sdmp, OperaGXSetup.exe, 00000008.00000002.2872841518.0000000001080000.00000040.00000001.01000000.00000008.sdmp, OperaGXSetup.exe, 00000009.00000002.2880101734.000000001080000.00000040.00000001.01000000.00000008.sdmp, Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe, 0000000A.00000003.2362613101.0000000003384000.00000004.00000020.00020000.00000000.sdmp, Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe, 0000000A.00000003.2362613101.00000000034F1000.00000004.00000020.00020000.00000000.sdmp, assistant_installer.exe, 0000000B.00000002.2365475236.0000000000447000.00000002.00000001.01000000.00000011.sdmp, assistant_installer.exe, 0000000C.00000002.2366144225.0000000000447000.00000002.00000001.01000000.00000011.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://partners-offapi.net/apiBundle/geo?sourceID=31120&subId_1=361D4F6E-6488-4FB2-BF8B-32AC8683517	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.1795740904.00000000007F0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://simpleflying.com/how-do-you-become-an-air-traffic-controller/	explorer.exe, 00000012.00000000.2713624554.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://addons.opera.com/extensions/download/0239ef3d7c95570d61b12b2fb509af435ccc2131/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.deezer.com/no/login	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.deezer.com/ro/login	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://completion.amazon.com/search/complete?q=	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://listen.tidal.com/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://desktop-netinstaller-sub.osp.opera.software/U	OperaGXSetup.exe, 00000005.00000002.2887132236.0000000001A0B000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gTUY	explorer.exe, 00000012.00000000.2713624554.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryera.software	OperaGXSetup.exe, 00000005.00000002.2887132236.00000000019D8000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://addons.opera.com/extensions/download/ad5beaae2fc679ccba1db1f7b3c9503d8da6ec70/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.remobjects.com/ps	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1777621493.00000000026A0000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1777988728.000000007FB40000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000000.1779494360.0000000004010000.00000020.00000001.01000000.00000004.sdmp	false	• URL Reputation: safe	unknown
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryve7	OperaGXSetup.exe, 00000005.00000002.2890562952.000000000502D000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2388096688.000000000502D000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2881045334.000000000502D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.innosetup.com/	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1777621493.00000000026A0000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1777988728.000000007FB40000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000000.1779494360.0000000004010000.00000020.00000001.01000000.00000004.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.deezer.com/fi/login	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://download3.operacdn.com/	OperaGXSetup.exe, 00000005.00000003.2167809590.0000000001A37000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2276745510.0000000001A37000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000002.2890562952.000000000502D000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000002.2887132236.0000000001988000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2388096688.000000000502D000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2881045334.000000000502D000.00000004.00000020.00020000.00000000.sdmp	false		high

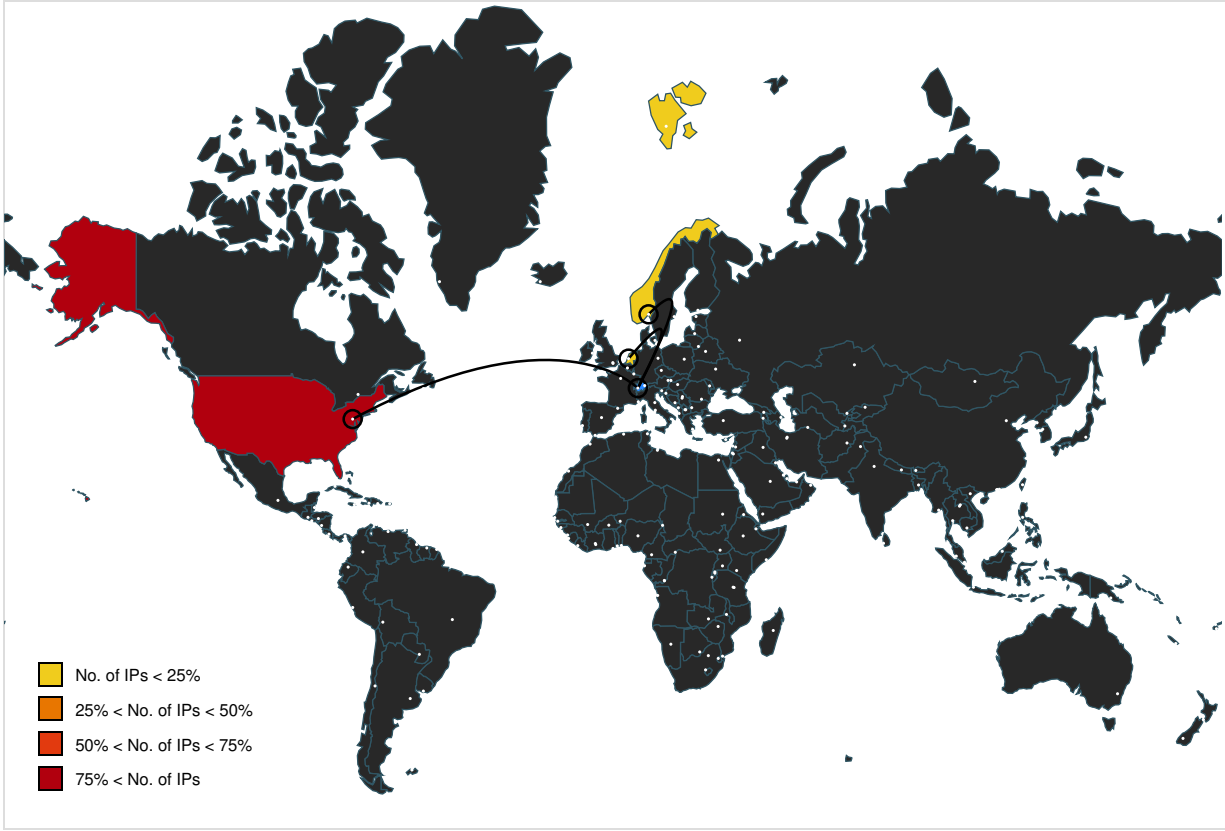
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://net.geo.opera.com:443	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2966678264.0000000003D47000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://download.opera.com/download/get/?id=52318&autoupdate=1&ni=1e	OperaGXSetup.exe, 00000005.00000002.2887132236.0000000001A0B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.so.com/favicon.ico	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.deezer.com/mx/login	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://wns.windows.com/L	explorer.exe, 00000012.00000000.2719255948.000000000C557000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://crashpad.chromium.org/	assistant_installer.exe, assistant_installer.exe, 0000000C.00000002.2366144225.0000000004047000.00000002.00000001.01000000.00000011.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false		high
http://https://addons.opera.com/en/extensions/details/dify-cashback/	launcher.exe, 0000001F.00000000.2765373482.00007FF6ED634000.00000002.00000001.01000000.00000017.sdmp	false		high
http://https://www.deezer.com	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://autoupdate.geo.opera.com/geolocation/	OperaGXSetup.exe, OperaGXSetup.exe, 00000009.00000002.2880101734.0000000001080000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false		high
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryCx	OperaGXSetup.exe, 00000005.00000003.2362601899.0000000001A64000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/?q=	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://yandex.com.tr/search/?clid=1669559&text=	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.kymoto.orgA	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2977724410.0000000002398000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://crashstats-collector.opera.com/collector/submit	installer.exe, 0000000F.00000002.2872788376.000002E63AC50000.00000004.00000020.00020000.00000000.sdmp, installer.exe, 0000000F.00000002.2875732136.00002B9C002AC000.00000004.00001000.00020000.00000000.sdmp, opera.exe, 00000021.00000003.2804768028.000073F0002E0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.kymoto.orgAbout	SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe, 00000000.00000003.1776639051.0000000002560000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2977724410.00000000023CA000.00000004.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.1782647300.0000000003490000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://assets.msn.com/weathermapdata/1/static/finance/1stparty/FinanceTaskbarIcons/Finance_Earnings	explorer.exe, 00000012.00000000.2713624554.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gHZu	explorer.exe, 00000012.00000000.2713624554.00000000078AD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://addons.opera.com/extensions/download/4d3d8f7f070d279fbe0d2795e10e69fbab5d3824/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/en-us/weather/topstories/us-weather-super-el-nino-to-bring-more-flooding-and-win	explorer.exe, 00000012.00000000.27136245 54.0000000007900000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://https://desktop-netinstaller-sub.osp.opera.software/6~	OperaGXSetup.exe, 00000005.00000003.2276 691379.0000000001A65000.00000004.0000002 0.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://opera.com/privacy	OperaGXSetup.exe, OperaGXSetup.exe, 0000 0009.00000002.2880101734.000000000108000 0.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00 007FF7097B7000.00000002.00000001.0100000 0.00000012.sdmp, installer.exe, 0000000F.00000002. 2877709511.00007FF7097B7000.00000002.000 00001.01000000.00000012.sdmp	false		high
http://www.kymoto.org	SecuriteInfo.com.Adware.Elemental.22.28512.27778.e xe, 00000000.00000003.1776639051.0000000 002560000.00000004.00001000.00020000.000 00000.sdmp, SecuriteInfo.com.Adware.Elemental.22.2 8512.27778.tmp, 00000001.00000003.297772 4410.00000000023CA000.00000004.00001000. 00020000.00000000.sdmp, SecuriteInfo.com .Adware.Elemental.22.28512.27778.tmp, 00 000001.00000003.1782647300.0000000003490 000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/politics/clarence-thomas-in-spotlight-as-supreme-court-delivers-blow-	explorer.exe, 00000012.00000000.27136245 54.0000000007900000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://https://www.opera.com/eula/computers	SecuriteInfo.com.Adware.Elemental.22.28512.27778.t mp, 00000001.00000003.2972553999.0000000 003690000.00000004.00001000.00020000.000 00000.sdmp, SecuriteInfo.com.Adware.Elemental.22.2 8512.27778.tmp, 00000001.00000003.182574 8633.0000000000864000.00000004.00000020. 00020000.00000000.sdmp, SecuriteInfo.com .Adware.Elemental.22.28512.27778.tmp, 00 000001.00000003.2964326998.0000000003E80 000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://gamemaker.io)	OperaGXSetup.exe, OperaGXSetup.exe, 0000 0009.00000002.2880101734.000000000105A00 0.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00 007FF7097B7000.00000002.00000001.0100000 0.00000012.sdmp, installer.exe, 0000000F.00000002. 2877709511.00007FF7097B7000.00000002.000 00001.01000000.00000012.sdmp	false	• Avira URL Cloud: safe	low
http://autoupdate-staging.services.ams.osa/v4/v5/netinstaller///windows/x64v2/Fetching	OperaGXSetup.exe, 00000005.00000002.2884 160745.0000000001080000.00000040.0000000 1.01000000.00000008.sdmp, OperaGXSetup.exe, 00000006.00000002.2895156720.0000000 001080000.00000040.00000001.01000000.000 00008.sdmp, OperaGXSetup.exe, 00000007.0 0000002.2146216434.0000000000A60000.0000 0040.00000001.01000000.0000000B.sdmp, Op eraGXSetup.exe, 00000008.00000002.287284 1518.0000000001080000.00000040.00000001. 01000000.00000008.sdmp, OperaGXSetup.exe, 00000009.00000002.2880101734.000000000 1080000.00000040.00000001.01000000.00000 008.sdmp, installer.exe, 0000000E.00000000.2683131 065.00007FF7097B7000.00000002.00000001.0 1000000.00000012.sdmp, installer.exe, 0000000F.000 00002.2877709511.00007FF7097B7000.000000 02.00000001.01000000.00000012.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.ico	installer.exe, 0000000E.00000003.2745278 631.000075B400604000.00000004.00001000.0 0020000.00000000.sdmp	false		high
http://https://www.google.com/favicon.ico	installer.exe, 0000000E.00000003.2745278 631.000075B400604000.00000004.00001000.0 0020000.00000000.sdmp	false		high
http://https://features.opera-api2.com/)l	OperaGXSetup.exe, 00000005.00000002.2890 469695.0000000004FF0000.00000004.0000002 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gMeu	explorer.exe, 00000012.00000000.27136245 54.0000000007900000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://crl4.digg	OperaGXSetup.exe, 00000005.00000002.2887 132236.0000000001A0B000.00000004.0000002 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://addons.opera.com/extensions/download/3ed7347a5e10c404ea6cb96281265ff23092cf8f/	installer.exe, 0000000E.00000003.2745278 631.000075B400604000.00000004.00001000.0 0020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://addons.opera.com/extensions/download/e27cf3ebc2172a1a7d9cb6978a031ef52ed55596/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://download3.operacdn.com/sp	OperaGXSetup.exe, 00000005.00000003.2167728563.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2276691379.0000000001A65000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.rd.com/list/polite-habits-campers-dislike/	explorer.exe, 00000012.00000000.2713624554.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://partners-offapi.net/apiBundle/stpstat	SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp, 00000001.00000003.2964326998.0000000003E80000.00000004.00001000.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.deezer.com/ru/login	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://addons.opera.com/extensions/download/434b0a6daa530638a964132e86b8a01d7b39aa7c/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://gamemaker.io/en/get.	OperaGXSetup.exe, OperaGXSetup.exe, 00000009.00000002.2880101734.000000000105A000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://addons.opera.com/extensions/download/aad01b6c6f7f2f01bea6584af044c96d8850f748/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://gamemaker.io	OperaGXSetup.exe, OperaGXSetup.exe, 00000009.00000002.2880101734.000000000105A000.00000040.00000001.01000000.00000008.sdmp, installer.exe, 0000000E.00000000.2683131065.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp, installer.exe, 0000000F.00000002.2877709511.00007FF7097B7000.00000002.00000001.01000000.00000012.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://autoupdate.geo.opera.com/api/prefs/?product=Opera%20GX&version=107.0.5045.79	OperaGXSetup.exe, 00000005.00000003.2388014507.0000000001A64000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2387970978.000000000509B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://addons.opera.com/extensions/download/313b7f796952f2b34bf6bce6ba10a7b51bd18913/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://translate.yandex.net/main/v2.92.1465389915/i/favicon.ico	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://addons.opera.com/extensions/download/505f20c0ceb331ebec9f6b8d9def5e0f59be4612/	installer.exe, 0000000E.00000003.2745278631.000075B400604000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binarytx	OperaGXSetup.exe, 00000005.00000003.2880727130.0000000001A64000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000002.2887654221.0000000001A64000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://outlook.com_	explorer.exe, 00000012.00000000.2719255948.000000000C5AA000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://browser-notifications.opera.com/api/v1/	Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe, 0000000A.00000003.2362613101.00000000034F1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://desktop-netinstaller-sub.osp.opera.software/v1/binaryBy	OperaGXSetup.exe, 00000005.00000003.2340456692.0000000001A64000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2880727130.0000000001A64000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2276691379.0000000001A65000.00000004.00000020.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000002.2887654221.0000000001A64000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.deezer.com/us/login	installer.exe, 0000000E.00000003.2745278 631.000075B400604000.00000004.00001000.0 0020000.00000000.sdmp	false		high
http://https://smolecular.icu/tfg/?src=setupIO	SecuriteInfo.com.Adware.Elemental.22.28512.27778.t mp, 00000001.00000003.2972553999.0000000 003690000.00000004.00001000.00020000.000 00000.sdmp, SecuriteInfo.com.Adware.Elemental.22.2 8512.27778.tmp, 00000001.00000003.182574 8633.0000000000864000.00000004.00000020. 00020000.00000000.sdmp, SecuriteInfo.com .Adware.Elemental.22.28512.27778.tmp, 00 000001.00000003.2968654031.000000000086E 000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.Adware.Elemental.22.28512.2 7778.tmp, 00000001.00000003.2964326998.0 000000003E80000.00000004.00001000.000200 00.00000000.sdmp, SecuriteInfo.com.Adwar e.Elemental.22.28512.27778.tmp, 00000001 .00000003.2985134000.000000000086E000.00 000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://download.opera.com/download/get/?id=52318&autoupdate=1&ni=1%	OperaGXSetup.exe, 00000005.00000003.2362 601899.0000000001A36000.00000004.0000002 0.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/world/agostini-krausz-and-l-huillier-win-physics-nobel-for-looking-at	explorer.exe, 00000012.00000000.27136245 54.0000000007900000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://https://autoupdate.geo.opera.com/https://autoupdate.geo.opera.com/geolocation/OperaDesktopGXhttps://	OperaGXSetup.exe, 00000005.00000002.2884 160745.0000000001080000.00000040.0000000 1.01000000.00000008.sdmp, OperaGXSetup.exe, 00000006.00000002.2895156720.0000000 001080000.00000040.00000001.01000000.000 00008.sdmp, OperaGXSetup.exe, 00000007.0 0000002.2146216434.0000000000A60000.0000 0040.00000001.01000000.0000000B.sdmp, Op eraGXSetup.exe, 00000008.00000002.287284 1518.0000000001080000.00000040.00000001. 01000000.00000008.sdmp, OperaGXSetup.exe, 00000009.00000002.2880101734.000000000 1080000.00000040.00000001.01000000.00000 008.sdmp, installer.exe, 0000000E.00000000.2683131 065.00007FF7097B7000.00000002.00000001.0 1000000.00000012.sdmp, installer.exe, 0000000F.000 00002.2877709511.00007FF7097B7000.000000 02.00000001.01000000.00000012.sdmp	false		high
http://https://crashstats-collector.opera.com/collector/submit0x300	OperaGXSetup.exe, 00000009.00000002.2884 935461.0000000028C24000.00000004.0000100 0.00020000.00000000.sdmp	false		high
http://https://crashstats-collector.opera.com/collector/submit--url=https://crashstats-collector.opera.com/	installer.exe, 0000000F.00000002.2875896 318.00002B9C002C4000.00000004.00001000.0 0020000.00000000.sdmp	false		high
http://https://desktop-netinstaller-sub.osp.opera.software/r-sub.osp.opera.software/	OperaGXSetup.exe, 00000005.00000002.2887 132236.00000000019D8000.00000004.0000002 0.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.deezer.com/es/login	installer.exe, 0000000E.00000003.2745278 631.000075B400604000.00000004.00001000.0 0020000.00000000.sdmp	false		high
http://https://autoupdate.geo.opera.com/api/prefs/?product=Opera%20GX&version=107.0.5045.79As	OperaGXSetup.exe, 00000005.00000003.2880 727130.0000000001A64000.00000004.0000002 0.00020000.00000000.sdmp, OperaGXSetup.exe, 00000005.00000003.2388014507.0000000 001A64000.00000004.00000020.00020000.000 00000.sdmp, OperaGXSetup.exe, 00000005.0 0000002.2887654221.0000000001A64000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://https://config.gx.games/	OperaGXSetup.exe, 00000005.00000002.2887 132236.00000000019D8000.00000004.0000002 0.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.deezer.com/de/login	installer.exe, 0000000E.00000003.2745278 631.000075B400604000.00000004.00001000.0 0020000.00000000.sdmp	false		high
http://https://download.opera.com/download/get/?id=65442&autoupdate=1&ni=1&stream=stable&utm_campaign=PWN_U	OperaGXSetup.exe, 00000005.00000003.2276 691379.0000000001A4B000.00000004.0000002 0.00020000.00000000.sdmp	false		high
http://https://www.deezer.com/th/login	installer.exe, 0000000E.00000003.2745278 631.000075B400604000.00000004.00001000.0 0020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
44.217.103.196	unknown	United States		14618	AMAZON-AESUS	false
37.228.108.133	unknown	Norway		39832	NO-OPERANO	false
23.48.203.201	unknown	United States		24319	AKAMAI-TYO-APAkamaiTechnologiesTokyoASNSG	false
104.18.8.172	unknown	United States		13335	CLOUDFLARENETUS	false
88.208.5.115	unknown	Netherlands		39572	ADVANCEDHOSTERS-ASNL	false
192.229.211.108	unknown	United States		15133	EDGECASTUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.10.89	unknown	United States		13335	CLOUDFLARENETUS	false
107.167.110.218	unknown	United States		21837	OPERASOFTWAREUS	false
107.167.110.211	unknown	United States		21837	OPERASOFTWAREUS	false
107.167.125.189	unknown	United States		21837	OPERASOFTWAREUS	false
107.167.96.31	unknown	United States		53755	IOFLOODUS	false

Private

IP
192.168.2.4

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1417615
Start date and time:	2024-03-29 19:34:13 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 14m 34s
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

Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	16
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:	sus38.rans.spyw.evad.winEXE@106/1185@0/13
EGA Information:	• Successful, ratio: 37.5%
HCA Information:	• Successful, ratio: 64% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, WMIADAP.exe, SIHClient.exe, conhost.exe
- Created / dropped Files have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- 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
18:36:53	Task Scheduler	Run new task: Opera GX scheduled Autoupdate 1711737405 path: C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe s>--scheduledautoupdate $(Arg0)

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-U02B5.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
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..380115120000Z0b1.0...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-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	3.06077288271926
Encrypted:	false
SSDEEP:	6:kKP5LDcJgjcalgRAOAUSW0PTKDXMOXISKlUp:X5LYS4tWOxSW0PAMsZp
MD5:	65E66C643C62F9356D9BDE3A2D8B6DA7
SHA1:	A69AF4850B203D2A220538A9CA2B89101C86A6EF
SHA-256:	06272A71D4E08484A18C6A748D559AA96C8FE3E9B5C82C9BEF53A7D2BE419DF4
SHA-512:	BAC58E5BB55C94CE1923E2D5BF75647CC87A281934E1143EF4615CCE019B2EA0191DE27BB610A354A77651C847D8B85BAA8CC13B442139D3EE7597BD1C713E85
Malicious:	false
Preview:	p..... ....l....l.....(..... .....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.ver0x000000000000002d.db

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	109624
Entropy (8bit):	4.024022148317409
Encrypted:	false

SSDEEP:	768:bP7FDIkDk2XGu/f5Njk0ygGPHjhd/N/LyrrJEn5KxQ6RR1v/0oVeXmcypJ3Mdhg1:Hk2/BG/VdSchgiPGjnf+PFYKJq/
MD5:	90477A9375ED2F730FE986BDC72A3218
SHA1:	FD720DA1DF06A7DFB9B2700F6800CA53CEF1DDF4
SHA-256:	6DBDBEAA611DF6225F82844424985D01D9DC3E891F9E2CC301136ECCB3A1B257
SHA-512:	A840922E947D6496C8A487C6D01F033BF1E34FE704C862ADEA10FE4B61D7564A516A2BE42BA4A82BC756B72B1B9C3663178AD1D8091236666B13EA8C45A011A3
Malicious:	false
Preview:	....h... ...8.........P.............Z...8...a.......... ....X.......e.n.-.C.H.;.e.n.-.G.B.............P.O. .:i.....+00.../C:\.....P.1..........Users.<..... ......U.s.e.r.s.....P.1..........user.<.....j.o.n.e.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.....P.1..........user.<.....j.o.n.e.s

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x000000000000002e.db

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	107824
Entropy (8bit):	4.037579683480944
Encrypted:	false
SSDEEP:	768:LDZF4tuykTGJzuFvPjk0m5OyhSwrvBGNGLw1eJQ+aoxZz8R1vIhokb1m/ypu3a86:Ak6uscyQsvzKhginGJnoUFkKeIphH
MD5:	4FDB20C57754C47432BBC293B4D8F4AA
SHA1:	151B795E6744B9D6C57A2B7455BCF3833E1BCB4E
SHA-256:	0A662BAB85975AF388647AAD2C7FB18EF5F5BF7D48A1C2D42D49571B092050BB
SHA-512:	8E5F454DCB4128104F24DEFED3561523D007305A6894DEC6F112FFA0506803D86C7D90769093B21643AD55F908665C3D91E35F5A594715D0763D5C194C687710
Malicious:	false
Preview:	....h... ...0.........P.............Z...8...a.......... ....X.......e.n.-.C.H.;.e.n.-.G.B.............P.O. .:i.....+00.../C:\.....P.1..........Users.<..... ......U.s.e.r.s.....P.1..........user.<.....j.o.n.e.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.....P.1..........user.<.....j.o.n.e.s

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x000000000000002f.db

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	105952
Entropy (8bit):	4.051217656460597
Encrypted:	false
SSDEEP:	1536:7kifyyupcojuiqzGh8iGGMngCF0KJXXSmw:7kgyyupcojuNzGh8iRCFznS3
MD5:	36A48CF290B28F3CCD11414CF62DCC69
SHA1:	973568BFDA3B8E7AFFECAADBDDA6EB60C1EC58D2
SHA-256:	72368748851A5B5710B4842489BD0F7132756CAA6DA5A971066D0573C1A5C3AA
SHA-512:	C4869F7AC79CB62B9990B9E742CE4381361D24A197576CBAC8D7BD817C1CF609EF2622E5123F11C04140138D6DA9D56E9E8E24743C9577B2B8A2F2785E2C576
Malicious:	false
Preview:	....h... ..............P.............Z.....a...0.............x...X.......e.n.-.C.H.;.e.n.-.G.B.............P.............P.O. .:i.....+00.../C:\.....P.1..........Users.<..... ......U.s.e.r.s.....P.1..........user.<.....j.o.n.e.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.....P.1..........user.<.....j.o.n.e.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\features[1].json

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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
Preview:	{"features":{"01979299c8cd":{"state":"enabled"},"13e025f64bd6":{"state":"disabled"},"13eeaf851da7":{"state":"enabled"},"15322f489976":{"state":"enabled"},"1ad69b007ce5":{"state":"enabled"},"1c4dddb65bac":{"state":"enabled"},"1d24dceb937a":{"state":"enabled"},"278deecb29a1":{"state":"enabled"},"2c1429a5a72e":{"state":"enabled"},"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"},"818c3ef12d0b":{"state":"enabled","dna_filter":{"required_dna":["64336fb81a04836eb8108d24fbca3aa3682db0a5"],"forbidden_dna":["5b3eb4a6c335a0659d16d1a189ca155e4441ea14"]}},"8511df77ed15":{"state":"enabled"},"970fe421a344":{"state":"enabled"},"9ec4e68ae70a":{"state":"disabled"},"b2a2a32b832b":{"state":"enabled"},"b7751444d14a":{"state":"enabled"},"b9677b

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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
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\ZJCZETOO\1698947853-custom_partner_content[1].json

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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
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\ZVZFKMB9\Opera_GX_107.0.5045.79_Autoupdate_x64[1].exe

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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/OocWSqlsw6I3iYwiA1+ulOYZ:gP4Z0/jl0vVB+usg
MD5:	E5C66BC2A10855CB4164EEF86F92FB0D
SHA1:	9453AA10DE00E311EE3415D1C07F1990FE6FB491
SHA-256:	FD238E7993A9800F8B9D5C0C0F4FB90E624823BC4A085F658F9544296A4A967D
SHA-512:	CFE5614CD7FBA269DC89A69240382B42649AA45449266447EC29E95A01C69D898F317AD75E07651BD75AB7FCF42C1E6E1731457F91A51397810744D95F1F96B9

Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ`.....@.....`.....!..L.!Require Windows..$PE..L...'..P.....(...F.....-.....@....@.....z.....b.....X.y..).....@..d.....text....&.....(..... ..`.rdata...5...@...6...*.....@..@.data....).....`.....@....rsrc..h.....@..@.....U..`.A.....S3.;.VWt.f9.b.A.t...`.A.P....P.|..Y.nj'.v....u..v..=.BA..6P.....P....9^..].v8.^..3.....hhDA.P.....P.....P..pAA..E..E....;F.r.....P.J\|..Y.24..j...lAA...t$..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\107.0.5045.79.manifest

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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
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-U02B5.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:	21ECE0DCF17B038400D09565438FCE8BE61746DAA0250F2FA9D0526BBA3D1CE6F8DA5CCE944EF8FA685C5EB6CF857B073D2A50ADA44A44A76D84813871FAAD0
Malicious:	false
Preview:	.PNG.....IHDR.....<.q....LIDATx...1..... ..6.^`.....{.....m.m].m.m.m.....[s...._.....N.Nw..._w..P...R... .....`....._[.i1...`.$.....C.....*.,...v.l.>.ZP.B...E@.....!?d..!.d.R.....g)0...^H[.u.4.k`....0<.d.1.....0...Q`..l.._T..!...\|pG.m=..a&.e.U(...C...n.^`.....FB.X...Oio...z!...:.Tx.8;..9.[a.....{.~.^.....P.].r..d..A...?....<y.v".....l.....^..._.....MA.o....?.>u._.d..`.....E.@.5.....E.....R...A..O){.k..2.....jx\..5U.a.%."#.nA....6.!..W2.....R..j6r..v...."....N.GA..8.....>..p..#..,X.....Q...y..#.a..)....Q.e.zc\.'@.Al.....io....=.....D.....F.....A#6.^.^.Ma5...b.b...D...+.P.. .[.o..z....,...#<U.0.O.#..Z.....Q{...jA..ka\|}...q.s.y^.!.Gh..R....t.g....F.....gt..6...7YjaU....0.*.....3..l.#.. =.h0t.06.v..C...T.}m..%...g..i,Cq..8.g.q..hx. .>..Kz...1....VF.)..q..$....._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-U02B5.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:	6A5E4105CCBE1664546798DB057B93622C9CBD6D5AF4967E6BE4E390A18FEC0FFCC807E3331F09ED0DE63ED85569BE7EC5EED5A7C663DF6CE4A5B70E09500371
Malicious:	false
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.#..~.$.7.]..Tm.....i.....+....m...x.j_.'"NG.]..n.j.v\{..Ls...;.T.=E..3...1;.v..xB...*"^.1U..8...xL,7]...D.9.i..".N..".....c..D...X...c+.t..8M...[.....".f.....R..0R.1..Xh..;ND.=U.ID.a.....v..8...'.uct.....k.q>.q.jc.+b...F....r....AN.....}.....Y.J.k~.;4.3".U....s..$....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-U02B5.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
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.$...Ax.....B....c.ih....G6L.....;...T.U0...l....~...........W....=<j.....X..O.....r.Y..-..Q..1.....q`..PC..jL...x.'9........y.b=L.m..(U........a.....W......`:.Me.jh..U0.......;..{..I..\|.W..C..4...b.nt.......L..a.........`9.!..7N@.......E.?..$.._.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...;.bjh..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-U02B5.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
Preview:	.PNG........IHDR...............V....*IDATx...{.]U}......"... .!.#..D .k..:.....5...6B..Q@+..lq.(%my.P..C-..Eb..<L5..<C!.1.$wu...f..}........5..Yk...^{.}..RJ)..RJ)..RJ)..RJ)..RJ)..RJ)..RJ)..RJ)u.d.Y.b?t..Q.E.,u......$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-U02B5.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
Preview:	.PNG........IHDR.............Oo......PLTE.....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-U02B5.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:	3B3E5BAF3CFC57119E0812DE2816DF6C7DCB42E96C4891E47C4F32320FD3BE2F27A0118051A6651595BAAAA30069BB1C0D78AA701744A44534CABE7547D4BECD
Malicious:	false
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. .l M2s5.==.%..-....|.:,.`.....<.c-.".\....I...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-U02B5.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
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.I./.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-U02B5.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:	F619D963B62EDB07C8077C3C6AE60ED8D3F3DD5BB1D05A2B83DCA1A7A4A346598B055F6C7EA22E05BF281B1DE0F205F5D1054819000759D9450EE1FE8F6491E
Malicious:	false
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.&.lJ.....|.....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-U02B5.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:	71940B8431E36307BA5176939A169B9259BB6B43C32529A10A12C5EA31447BDDCCAD7EB9EF7CB309B175EE7BD56E70926BD5AA0855D0FD9497547ECD7FF9315 8
Malicious:	false
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....I...,...$7.....0,%.. ..l[Au"...d&?.j.....,..|...~F..pB...]......L.]d.v5...U%..h:}%..._$...X.m.....S.yL...Bc.R;K..8...*..TiP.}5.g..p..m..s].ZU....H.{P.!,..?......t.U....=m-<.a.v..I$...u.T5..LG..b]...c6.19d;k%.. .3.....,..I.[.1..:...YN...h.*5...W..._....dL6.v.Rch..~...i.1G....|].AU.k...H.[Q.a,6.5-....Gt.9U.....n(.#...D.v....._.*...@I.}...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-U02B5.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:vHNfCYvjHq3yow73tnF7H1r8IR07iBa/ptAFjLmocqM3LNpi+MaG9vz:vHsY7Hq3QzT7H1r8Wr0/zAxfyLNp1Pab
MD5:	504D80D276ADCC0163A8E4720013F9E7
SHA1:	6D34A0593FFCE916CD19B66D61004FD7E7EB2CD1
SHA-256:	EBBE0B4761EA8968A0A3FAFB383AC7AE175E98CD31A0F41BDF5FCB43469B58EC
SHA-512:	9961259704FF97C0E1899A33259F62155B73264E272064F3FA90E64124513C7C8BD6AB69A39C1EFB271ECC2972AB8FD86FB836F22153A9BB35419C3816D11337
Malicious:	false
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.<."""""|%.J..2.L...xFp?...?.8....:N.M..`2.i. .M.uZZ+'..C......9.f.1.X.}He....b...$..V..'..T.....[.s..}..F.....t.lnK..d.5...Yr..ld..x.\...iP... ....X.....a ...i.C.D.E.H.&.....Y....h..G.....1..h..C..>t...$...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-U02B5.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:FtyHJuovwDhIXRvUCvqfPAuwdESKbtU04aQkClnRU8lbPxbsFlV4hEIA:FtygGwDhIX1oHO4KwCAQ9MEIA
MD5:	667BFBAAEB2D2B372B6E0D4BF4992CE4
SHA1:	4C6C2E07183963F59391945FBEE077B55F8F6B2A
SHA-256:	207519F1C7B6C7509BFEB7B55724997EEC6456C8BAF55E882E72FC5CD43DA221
SHA-512:	AC63A3DD2F6088E7849E3824C35FD58CA78EC77DC31E1F6CBD47DE7CC394318CBA7D2309912206A94180267BE057C2AF5C835424019E2A03EE33A2AB801BA9 4
Malicious:	false
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..$..R9.....&..NMW..{..4}.....m....h..y/..x....a.[e..7.ua.^.IC8....I0....1...r.&.....G.....c.....d....F]...M.a&.M..V..?[..t.P.Xx...*<.(...s...'.Q....'.~{_.....8....R.%..7|O.BI..... Sr....^..@.....us.".M..?x....*.T.....A....&.I.....H`g..."...I}E.7..]..=...C.gz.....V!.EE.....7WvB.!.d..vJ...k.{?.....1.n/.Q.{.....LD..;k...\....]G..S.+....F3.}z.=F(.....$..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...!v..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-U02B5.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
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-U02B5.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
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.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....l-.l..+...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-U02B5.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
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...,,lc"-.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;..)..ld.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?l....?.{...`5z3..w8.....s.B.d..K..K....LLY.j..^...a.p.~.z....-.....l.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-U02B5.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

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..`wI.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..'...I.-.?j^2..*~}Zo.J..7..F....D.91.....#2^..7.}7.....\$.:P..oc"6I..)n... |A..G.....I'..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-U02B5.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
Preview:	.PNG.....IHDR...8...8.....LIDATx...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-...[I.'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-U02B5.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
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-U02B5.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
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-U02B5.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
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-U02B5.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
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-U02B5.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
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\cb3aa22f-8954-4c6a-8828-0b23d4eea54f.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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
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\.'@.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.....g

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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:	B2C7F4FEB2D323DEC2455710F6B04EF9642803FEF02936DBE5A09FC00453F8CBE2CE2E93BA2E5CDE537DAF7342BB14D6C0D49D1700AE86C8C2310863E3FB338E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
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.....@....pdata.....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-U02B5.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:	44DA8661C4C6368FC046C99916B2109EB763B7D9EDBEA66B1EB70A651C018DEED91C8EE2F3269B10591ECFC082C85D43E6ECA555BEADBD1B83C898ABC1B2CCA5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
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-U02B5.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
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\files_list	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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/Rtp7yTf85XZyITJhowbO7VtiORFnbwU:Gaf85XMbwbOHiORFnbwU
MD5:	2DC8E2607CA1F7C321FB559287B7CA22
SHA1:	C1C7BF3A567FD2D24C348C3C954FEC3E00F96AEE
SHA-256:	269738732DC4756D0955EF9BBA7DE3A4DD025C0A868EE84E3FFC486817F63672
SHA-512:	080FD30D024EC21B7E50BBDB2FFD69E7E700B2D923171BFC2E47C77E510D663F5DAAFD702017A61C6D399E17705678E182D5F0BF53505181D864F533EEA22FD 1
Malicious:	false
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-B lack.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-E xtraLightItalic.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-Se miBold.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.1711737405.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/Rtp7yTf85XZyITJhowbO7VtiORFnbwU:Gaf85XMbwbOHiORFnbwU
MD5:	2DC8E2607CA1F7C321FB559287B7CA22
SHA1:	C1C7BF3A567FD2D24C348C3C954FEC3E00F96AEE
SHA-256:	269738732DC4756D0955EF9BBA7DE3A4DD025C0A868EE84E3FFC486817F63672
SHA-512:	080FD30D024EC21B7E50BBDB2FFD69E7E700B2D923171BFC2E47C77E510D663F5DAAFD702017A61C6D399E17705678E182D5F0BF53505181D864F533EEA22FD 1
Malicious:	false
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-B lack.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-E xtraLightItalic.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-Se miBold.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-U02B5.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:s3uV82wWqsPziK4zbOPb96DNAV8
MD5:	4154321279162CEAC54088ECA13D3E59
SHA1:	5E5D8C866C2A7ABFD14A12DF505C4C419A2A56F7
SHA-256:	6BDEBEB76083E187C7AE59420BFC24E851EDB572E1A8D97C1C37B7B2DC26148C
SHA-512:	04CA175774CBE3F2D83543C01CC388E2715AB7B1378143DB41BACDC7E7EDDF05D3BEEF476F6ACBE7DDEB34861984EFB5FD7F299EC1820697C440B372D258AEE7
Malicious:	false
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-U02B5.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
Preview:	.....GDEFj.`i.....GPOS2-.....?4GSUB*|.@..D<..[.OS/2 .B...,...`cmap^.....d.cvt O._..a....&fpgmb/....b.....gasp.....a|....glyf5.....|.head0;.`...4...6hhea.....l...$hmtx ..4.....-$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-U02B5.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+6l/8
MD5:	8F2869A84AD71F156A17BB66611EBE22
SHA1:	0325B9B3992FA2FDC9C715730A33135696C68A39
SHA-256:	0CB1BC1335372D9E3A0CF6F5311C7CCE87AF90D2A777FDEEC18BE605A2A70BC1
SHA-512:	3D4315D591DCF7609C15B3E32BCC234659FCDBE4BE24AEF5DBA4AD248AD42FD9AB082250244F99DC801EC21575B7400AACE50A1E8834D5C33404E76A0CAAC834
Malicious:	false
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.....!...#

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-BoldItalic.ttf	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.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
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....$hmt x...T..y<..-$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-U02B5.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-a5213159 5;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:	65875F9F205CD70D2E1B86FBDA2AC8875637E0B3E0BB37ADE9DA20717B0F17D2108A0CF2AA1B246AFFD73BEA233B510D37D13193801D94E5148D3EC4159653E C
Malicious:	false
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.....l...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-U02B5.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
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-U02B5.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:	67808D6BDAFE9BCF5576DF234C93611BC827D868DD9F0D064E801DDA5EFE67883637746458B3A0E51B4B394913C3AC47F56C5C055B3FF013ABEBB66EC9A771F
Malicious:	false
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.....xprepIdhL..@.....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-U02B5.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
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[.<.....}.prepIdhL..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-U02B5.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
Preview:	.....GDEFj.`i.....GPOS.}.....7.GSUB*|.@..<...[.OS/2.....`cmap^.....d.cvt H.6..<....&fpgmb/....=.....gasp.....<x....glyf....._Lhead0..i..\....6hhea.?....]....$hmtxF)...],..- $loca.k6....P..-(maxp.D.....x... name.....>postzz.{.....}.prepIdhL..K.....*...,.....;...>.H...J.X...[.]..._.`...b.y...{..... ...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.\|...~..... ...".$...,.,.....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.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\fonts\Inter-Light.ttf	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 39 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter LightRegular4.000;git-a52131595;RS MS;Inter-LightIn
Category:	dropped
Size (bytes):	408364
Entropy (8bit):	6.1740190502785195
Encrypted:	false
SSDEEP:	6144:oeroPfXwF22mZ8JWPziKSQYfW0LXYveHt+47O3YqF5nxeU2h8jjXVymj3k4yhb18:ovw22mZzPziKYW0jYves4I2n8
MD5:	FF5FDC6F42C720A3EBD7B60F6D605888

SHA1:	460C18DDF24846E3D8792D440FD9A750503AEF1B
SHA-256:	1936D24CB0F4CE7006E08C6EF4243D2E42A7B45F2249F8FE54D92F76A317DFD1
SHA-512:	D3D333B1627D597C83A321A3DACA38DF63EA0F7CAB716006935905B8170379EC2AAB26CB7FFC7B539CA272CF7FB7937198AEE6DB3411077BEDF3D2B920D078A3
Malicious:	false
Preview:	.....GDEF.m.v.....GPOS,F.P... ..=<GSUB..B..B\..]@OS/2...2.....`cmapL.....d.cvt F..,..*....&fpgmb/....,$....gasp.....*.....glyf:;.....B.head0....G....6hhea.....G....$hmtx ..Zi..H ..-.loca.&9...u...-.maxp.t..... name..-.....post}U.7...|...xprepldhL..:0.....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-LightItalic.ttf	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 38 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter LightItalic4.000;git-a52131595;RSMS;Inter-LightIta
Category:	dropped
Size (bytes):	415024
Entropy (8bit):	6.199271793956543
Encrypted:	false
SSDEEP:	6144:BgWQyjl8Ai+XWqSBxVUW+EuzZKKH+XgoniJ2D5L2kZSVbnN90oGPP3+4yCT18:BgWQtiiWqgsR3n+XgZJ2xqu58
MD5:	4B1FFAD3C0075AF22674765FF1EE2F56
SHA1:	1F7B05D0ED1C6C15736115A59AD844ADEA5F1F66
SHA-256:	FE3714926082AC5764327E3B67AE52CB6F0CF6B8C4221C064A6CACF821079414
SHA-512:	427DB3FE5860676FAB65A9B895D205620A1EC0AA172F45AA9ECEF261820E25B84F3413BC5D0A9D0C1311422A8DA1F5706AC4F6211A60AACC82974CF00FF036A4
Malicious:	false
Preview:	.....GDEFj.`i.....GPOS...C.....;\GSUB*|.@..@d..[.OS/2...S...T...`cmap^.....d.cvt F..$..E....&fpgmb/....F(....gasp.....D.....glyf..t....D..clhead1 ...d....6hhea.i....d....$hmtxU.b...e...-$loca.....0..-(maxp.D.....X... name!A-....x....postzj.\...X..}.prepldhL..T4.....*...,.....:...>.H...J.X...[.]..._`... b.y...{...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.\|...~..... ...".$...,..... ..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-Medium.ttf	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 39 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter MediumRegular4.000;git-a52131595;RSMS;Inter-Medium
Category:	dropped
Size (bytes):	411500
Entropy (8bit):	6.179950752404769
Encrypted:	false
SSDEEP:	6144:D0RV3jlWkDOh9oC2wuhsJWPziKSQlRiFy34YmkCD9ol0+msvMlwt5BO2x28YzWDQ:D9SxC2wuhDPziK2yIYmkCCIPmsHI8F8
MD5:	A473E623AF12065B4B9CB8DB4068FB9C
SHA1:	126D31D9FBB0D742763C266A1C2ACE71B106E34A
SHA-256:	1BDA81124D6AE26ED16A7201E2BD93766AF5A3B14FAF79EEA14D191EBBD41146
SHA-512:	1FBC2841783140FE54F3AB1FA84E1DED2534BCEC3549ADE2F513491B32178DF515BD63A0A4A2C35017A6850FF9C3A24F8602357D912ACF8CA92B8D68BA846D3A
Malicious:	false
Preview:	.....GDEF.m.v.....GPOS@@..... ..J.GSUB..B..O...]@OS/2.P.....`cmapL.....d..d.cvt J"....7<...&fpgmb/....8d....gasp.....74....glyf.....L..A.head0....S....6hhea.c....T 0...$hmtx.....TT..-.loca.....-.maxp.t..... name ./.....post}m.g.....xprepldhL..Fp.....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-MediumItalic.ttf	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 38 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter MediumItalic4.000;git-a52131595;RSMS;Inter-MediumI
Category:	dropped
Size (bytes):	417780
Entropy (8bit):	6.206431815755074
Encrypted:	false
SSDEEP:	6144:/DRFemw/pjVeXWqSBpVUW8KOA8HiQ109P0GJrMfsVwGSkSdnMgVlwZp3+4yCr18:/DKmChCWqgkJKy6zMfsdUDv8
MD5:	9A21378C7E8B26BC0C894402BFD5108C
SHA1:	72BD9F3CA75CA691CE86FE1EBBDB269F5F737BAE

SHA-256:	0D34F9588400A586B774BE97E66AE8C076A8807B8455DF0587B39D2A4A1A3B42
SHA-512:	4A9D23A01F1A7474E0339D4D8B151D0269BFAF7D9E13FF6AA34D7F929002E8FF185F273E6F7AFD2D40DF3E0630A962DC7767D870DCF1766F3E04B8029A7B452
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOSNc.....H2GSUB*|.@..M<..[.OS/2.Q.....,...`cmap^.....d.cvt J..}..O....&fpgmb/....P.....gasp.....O.....glyf...Y.....aLhead0....oh...6hhea..... .o....$hmtx.....o...-$loca.l.....-(maxp.D..... name#..y...0....postz.....}.prepldhL..^.....*...,.....;...>.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-Regular.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 35 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInterRegular4.000;git-a52131595;RSMS;Inter-RegularInter
Category:	dropped
Size (bytes):	407056
Entropy (8bit):	6.1736927573676335
Encrypted:	false
SSDEEP:	6144:sSnv4IXwF22mZ8JWPziKSQUmeKGVOOxAdgwH9evDFDynor51EOO2UAGbzxSr1w7b:sSvJ22mZzPziKwLOOkvH9IQoUf7P08
MD5:	FDB50E0D48CDCF775FA1AC0DC3C33BD4
SHA1:	5C95E5D66572AECA303512BA41A8DDE0CEA92C80
SHA-256:	64F8BE6E55C37E32EF03DA99714BF3AA58B8F2099BFE4F759A7578E3B8291123
SHA-512:	20CE8100C96058D4E64A12D0817B7CE638CEC9F5D03651320EB6B9C3F47EE289CCC695BD3B5B6BF8E0867CDAB0EBB6E8CAE77DF054E185828A6A13F3733ED E53
Malicious:	false
Reputation:	unknown
Preview:	.....GDEF.m.v.....GPOS,ta.... ..9.GSUB..B..>...]@OS/2..g.....`cmapL.....p..d.cvt H.H..%....&fpgmb/....'.....gasp.....%.....glyf..L...X..A.head0..j..C....6hhea...]..C8 ...$hmtx.....C\..-.loca...X..q...-.maxp.t..... name...V.....npost}e.V...`...xprepldhL..5.....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-SemiBold.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 39 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter SemiBoldRegular4.000;git-a52131595;RSMS;Inter-Semi
Category:	dropped
Size (bytes):	413976
Entropy (8bit):	6.169175161562876
Encrypted:	false
SSDEEP:	12288:SMPc0C2wQtzPziKFfAi2bNru42U5CB1c8:5hiK9AiENr/2UYc8
MD5:	4D24F378E7F8656A5BCCB128265A6C3D
SHA1:	D48310D2F04C57AF1BCE0851E053BE7B58B25DCA
SHA-256:	0DC98E8AA59585394880F25AB89E6D915AD5134522E961B046CA51FAD3A18255
SHA-512:	38B18D9786046633E4992308C88F11CA5CED325F805EB29B3000533459E85DFB6CD87655F1E285AF8DA22AC04722AB354DBDA24667297B56CCA824EF227373F1
Malicious:	false
Reputation:	unknown
Preview:	.....GDEF.m.v.....GPOSd]..... ..KPGSUB..B..Pp..]@OS/2.....`cmapL.....d.cvt Kt....@....&fpgmb/....B.....gasp.....@.....glyf.8.....J.head0....]....6hhea.A.h..]....$hmtx{xJ...]...-.loca.!R.....-.maxp.t.....\... name%.1....\....post}v.w...h...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-SemiBoldItalic.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 38 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter SemiBoldItalic4.000;git-a52131595;RSMS;Inter-SemiB
Category:	dropped
Size (bytes):	418520
Entropy (8bit):	6.2010032658690255
Encrypted:	false
SSDEEP:	12288:0UW00H2WqgwJA65hgQ0Yp9nyu8qIzoGS9U8:FWwJAuGQ0Yp9n5szrlU8
MD5:	04551623D1023398FD3DA941E920D727
SHA1:	92789CCC0D76C04D86685F9F0529731D2DC38852

SHA-256:	1E1289453D7A895CFB73569D4851634C8B0E49D150C4DD52D44BF5D206908272
SHA-512:	8017346110AEE84614FC0D9A9B39505F042E23659BE367C8A84301DC6E41C3DD93A464E88DCDF06F10B3B3AC85E975BC69EB464ED4CD784309564836289D412
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOS..j.....I:GSUB*|.@..ND..[.OS/2.....4...`cmap^.....d.cvt K_....R....&fpgmb/....S.....gasp.....R.....glyf.....$..c.head0....r4...6hhea.....rl...$hmtx ..Q...r...-$loca.n.....-(maxp.D..... name(u0.....postz.....}.prepldhL..a.....*...;.....;...>.H...J.X...[.]..._.`...b.y...{.... ...../...1.1...3.7...9.R...T.T...V.W...Y.Z...\.c...e.|...~..... ...".$...,,..... .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-Thin.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 39 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter ThinRegular4.000;git-a52131595;RSMS;Inter-ThinInte
Category:	dropped
Size (bytes):	403404
Entropy (8bit):	6.15775244572357
Encrypted:	false
SSDEEP:	6144:FZbewyXwv22mZ8JWPziKSQQQbdiJNnL1qIPQyC4JRPeQQFgppInr/qwAWJBIF072:FZCU22mZzPziKPd6PQgcgpa/nMF07J8
MD5:	B97F16379B4C106616F60F702733F5C6
SHA1:	85C472FB9A7F256643BC4BBA10F158DFAA1D1E8B
SHA-256:	4C392DCC8AD916F0F9DF7559AB5563B01DD94F9F3B2DB34617FE392E00060339
SHA-512:	D124AF2C705B97CBB307497F88C47A5F7D320174D48626EA14AC27D42BCF8016F32810CF7ECB6AF1261297B8C331A6EA89E2E35C3E2536390D8D6E500ED8D61E
Malicious:	false
Reputation:	unknown
Preview:	.....GDEF.m.v.....GPOS..... ..6.GSUB..B..;...]@OS/2.....`cmapL.....L..d.cvt B.....&fpgmb/.....gasp.....glyf5?.$...4..6<head1..i..4p...6hhea...-..4....$hmtx. .6Y..4...-.loca.....b...-.maxp.t.....@... name..z...`....post}6.....xprepldhL..&.....l...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-ThinItalic.ttf

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	TrueType Font data, 17 tables, 1st "GDEF", 38 names, Microsoft, language 0x409, Copyright 2016 The Inter Project AuthorsInter ThinItalic4.000;git-a52131595;RSMS;Inter-ThinItali
Category:	dropped
Size (bytes):	410232
Entropy (8bit):	6.191384356621797
Encrypted:	false
SSDEEP:	6144:nm0XOI8wiWXWqSBNVUWI9Wd4EZDSwKBUMimozkhBiv98svLAYP0wJShe3+4yCL18:nm1GiqWqgwbMd4EZDDpmokGllkYMdQ8
MD5:	12EC66B825B504D752E8C333BF81DACF
SHA1:	56896D3E6011466B7E6631C714C57E20EE8366D9
SHA-256:	5FC09AF94A447FAE6F82C00F15DFAEF9EAE7C560E6CBE46D3E84524019A574AA
SHA-512:	8CB838589AC4F9819B7E2204517445DF94663D3217297212973E8B2D9FECE162155130DDC783E7E89EF2832D38BACE731B2AE3B73AFF36AD782C707813BC52B4
Malicious:	false
Reputation:	unknown
Preview:	.....GDEFj.`i.....GPOS.n.t.....6RGSUB*|.@..;\..[.OS/2.....L...`cmap^.....d.cvt B.....2H...&fpgmb/....3p....gasp.....2@....glyf.,.....<..U.head1<.h..R....6hhea..._. .R<...$hmtxt.<...R`..-$loca.?w.....-(maxp.D..... name..+.....postzK.....}.prepldhL..A|.....*...;.....;...>.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\headless_command_resources.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	2889
Entropy (8bit):	7.9306579237637775
Encrypted:	false
SSDEEP:	48:IGAlAoYphRTc/LR6nfEGlsX+bW+eeyYsO5EtDF3a8MnXULZACcb/+0TKw8uYsyKF:EcphRltAs43bW+ee6OiFMXqnoLT0NYis
MD5:	1F9CCBBBFC1E065FCE62137DAB8630B3
SHA1:	D653C3F32C11155B9F0B7DA1B7FAD78F4D3A22F9

SHA-256:	27B61CF817E6274437C8F9D22E03F05F3D78DB32A29D0DE7E0C39E642E78EF3F
SHA-512:	D37972843971A0D2BB1B06B8D059323E35CE449CCD89F08A8A87E938781430CC6DBFFB5FFB5500FE530B544118769F5378B8343CFE135B7AD640525A16B1E045
Malicious:	false
Reputation:	unknown
Preview:	.....m.....m.....I.....-.1k.0.....Kv....h....."=G*.^....Uqo9...R..1g.w..mqv..e.~.x...,+..[.<.8/...!.....6C..tTR.@..P.Xq....-_#O.....4`.P.....|...J.5.....~.8.6...p.:.. l.].l.Y._EY.....N.H....H...4&.>...%@.F.P..V.....].r.....6!.(mW....)..#.nh.X2.....j....U...-..v....#R"..:.....^.d.i..t.A.z;?.....r...[f..Y.n1.T..)P..:Fg.G'..'..j...6.8:.<.+.0...Y. .%....s.1...8.+HH.....c..:D/....w].h...;t..q.....4.)f=m...i....\...y_...3.0.....|fH.....%.0V.n...6c.....W.W...Dj...O.30....i.....8.....H..J.o.P.)2U.BC!M5..X.T...$.-..R...8C..j... . .fb9. ..Aa.....X.....v,.._4c.k..qJ.... .4Z^.*pe..@..g.]9..x.....n".....n..v!.'..[.. _4.^...YS.vS@-%..6!..r..4.1P....!.....5<.....)....0.....B:.G,="..M..y..8".....q1C@7[u.tn.....#...UE.o..P$...f. I."....f6...1.e.8..+B.N..Q. ..fQ...<$.).....D....kQ..m...K(.....sZ)...6-.C..<<DQ.n1...4..L/c+_.....Kr4.....Q:H....H=...-._>A..."h.(.....@.

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	1028288
Entropy (8bit):	7.978101123188429
Encrypted:	false
SSDEEP:	24576:3SHKqVVG7/dOMJlcFDAh1y+cBtoO0TOxuGtY1waxNU:CHKyG7/dR2ZpHBKOxA1C
MD5:	03F57C15087DB4F21D3F1CA51A2D26D3
SHA1:	74F44C7870F87CA82B670D8EE3B4F891D6390F3D
SHA-256:	281152795AC7FF1993729468D45EED78B724F886AFAD24528DE2EED240A66C4F
SHA-512:	FD728E9A8E988F01AF5999AC165CD0745A1F605F217D81FFE7A338FC0EDA60C8D76E572E6945DB16409D355085C7EC00F341DAA032C4204EFC789E169F129BE
Malicious:	false
Reputation:	unknown
Preview:	.....u...f.0.....C.....)....%.....<.....4.....-.....w....n.....n.....nZ....n.....n,....n.....n.....n.....n.....n.....n.....n....n6....n\....n.....n.....n.....n.... .n(....n].....n.o...n,....n}....n....n.....n....n....n.....n.....n[....pR....p.....p.....p.....q.....r.....r9....r.....r.....r.....r.....r.....r.....r.....r.....r.....rX....r.....r.....rX....r.....r.....r.!...r #...ra%...rK&...r_*...r.0.. .r.6...r.6...rs;...r$>...rH?...r.@...r.A...r.B...r.D...rkK...r.L...rKP...r9\...r.^...r.j...r....r.....s.....s.....s\....s.....s&....sR....s.....s.....s.....s.....s.*...s.+...sx;...s.u...s2v...s.w...s.x...s.y... s.z...s0{...s.... s.....}.....}.....}.....}&....}.....}w....}^....}H....}=....}.....}.....}.....}.....}v....}P....}%....}.....}.....}w....}.....}U....}.....}.....}.....}.....}K....}.....}.....}U....})....}.....}.....} ....}.....}. ....}W....}.....}.....}_....}.....}.....}.....}.....}?....}.....}.....}.....}K....}H....}..

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	3148964
Entropy (8bit):	7.9797214008707
Encrypted:	false
SSDEEP:	49152:gubH3aVcrwso1yyrwz3yCo7X6sFiSMLbivc8qJKIRQ/u8SDEIHjcW/99w:gubH3aGRogyrwry9w9L2UYI2mB6
MD5:	A2A88F134B6A41245A7FD6881F2BFDA6
SHA1:	C55C6DA16E04AF692D39587C5F11BED31BF1EA07
SHA-256:	6F74802AF7F9F435D8853AA2131131751DE19FE7FFE91AFC7E203543D4E718C5
SHA-512:	D7BE69FCDFFD56FBFCC0C208AE5EA8A19FACF2E3A5AA1896A49155221A38D74A3C4441BDFDA9901FEEEBBE0B4231DF4D6B0DEE999D9D7F41858B5C3FD35E C071
Malicious:	false
Reputation:	unknown
Preview:	.....b.}....Rn...._n....qn.....n.....n.....o....fo.....o.....o.....p....dp.....p.....p.....q....dq.....q.....q.....r....Zr.....r.....r.....r..../s....Xs....fs.....s.....s.....t....&t....wt.....t.....t.....t....Vu.....u.....u.... .u....Hv.....v.....v.....v....$w....kw.....w.....w.....w....:x....fx....qx.....x....:y....\|y.....y.....y.....z....!z....0z....nz.....z.....z.....z.....z.....{....Q{....r{....~{.....{....&\|....X\|....k\|.....\|.....}.....}..../}....;}.....}.....} .....}.....}....E~.....~.....~.....~.....~.....~.....J.....s.....~.....9.....w.....<.....R.....\.....,.....s.....J.....e....t.....=.....M.....*. ....B.....\.....j.....&.....].....z.....H.....W.....i.....X.....$...../.....3.....:.....D.....I.....w..... .....

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	10750576
Entropy (8bit):	6.281341985010261
Encrypted:	false
SSDEEP:	196608:oQPBhORiuQwCliXUxbblHa93Whli6ZU6WOH:oMwkDliXUxbblHa93Whli6ZkI
MD5:	5784C2B7CA4736D45F771838D3DDA6E2
SHA1:	82A1CD2E1221044773ADDF27A32575DF6C06ADF1
SHA-256:	3A04D42D8C3149F2FC9350A16BDF2354FDDA46D68E3BA1ACE727E6DA2D98D17B

SHA-512:	5E465A22EA41658A9A910FDBCE276E805A2D6FD4D042750E96F3AB95A5C92C5EEAA76A160F745AA66B44AB8EB3FCC37FCFE5907AE19E16EE2FBB2C10CB82104B
Malicious:	false
Reputation:	unknown
Preview:	...'.....CmnD..... Copyright (C) 2016 and later: Unicode, Inc. and others. License & terms of use: http://www.unicode.org/copyright.html .....F.....,F...0..?F...1..RF...1..bF...9..uF...9...F...j...F..0k...F...k...F.....F.....F..0....F.....G.....G.....+G.....>G..`...QG.....dG..p...wG.....G.....G.....G.. ....G.....G..@....G..0....G.....H..@..."H.....5H.....HH.....[H.. ...nH.....H.....H..0....H.....H..@....H.....H.....H..@....I.....I.....%I..0...8I.....MI.....eI..@...zI.....I.....I..0....I.....I.....I..0....I.....I.....J...3..$J..`3..7J...3..GJ...g..ZJ...h..mJ..Pk..}J...k...J...k...J...M...J.....J...$'..J...0'..K..01'.+K.. 8'.EK..p8'.\K...@'.sK...A'..K..@F'..K...H'..K.. K'..K...X'..K....(..L....(.$L....).=L....).\L...Y*.~L....*..L.. -+..L....+..L....+..M...W,.7M..@.,.NM..0.,.IM....,..M....,..M....,..M....-..M..`g-..M...h-..N...T/..N.. ./.>N..p.0.UN....0.qN....0..N....0..N..P.0..N....0..N.. /0..N..p/0..N.../0..N...[0..O..@\0.$O..

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6949792
Entropy (8bit):	6.814706947908496
Encrypted:	false
SSDEEP:	98304:+g3JY5poHR/dVh6txfG1loZO4FSrn2vTjg:L3JY5pmR/sfGzoZ1Fs2I
MD5:	21AD4599ABD2E158DB5128F32D3CC4EE
SHA1:	64B4A4E84AB7E68BAD798643162B88CA4678338B
SHA-256:	F7CB5A7A18FE1102A2F591B6AD7B79C68C972742DE2F34691771C1E9BA6BD82D
SHA-512:	52F5F1B39F4887BA4EC31593F4392D0F8381CDBBD233A22CA2A326F34DFF446477334ED7D8F4C9DBD3462D60BB7021C52F4CE9920530BD7AE21C40BCFAEEBC17
Malicious:	**true**
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....."....."....d.....@.....pj.....j...`.....P.....b.....;....i..)...`j.(...|...8.....`...(.....@.....text..... ..`.rdata...d.....f.....@..@.data...PJ..... ...h.....@....pdata...;.....<.....@..@.00cfg..8.....@..@.gxfg...P&... ...(.....@..@.retplne.....P.....tls.....`.....@..._RDATA..\....p.....@..@.rsrc.....b.....b.....@..@.reloc..(....`j.....i.....@..B.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer_helper_64.exe

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	616864
Entropy (8bit):	6.224717035550476
Encrypted:	false
SSDEEP:	6144:N+AWKhweCwL/Xn5lKDdbJRgbOmAR7/XvNk1I/KY2Oiul8ohseUWdZT:N+AwwLvnPKDdYgRLvi1lJt8oudWdZT
MD5:	298D95DFE54364E5D864916D8B42B57B
SHA1:	9714235D3D26B46B35CE1F7FFEBC4D280591BB52
SHA-256:	03D73AF7132EB077586ECA4E0E6AF7BC60A04A01D241A3960093C290E302E73F
SHA-512:	629CAE4CF987EA91DA82B5CEE7AFED55B3D7FDA71ECBB12614FE4B3211B1F4B3321AE596D5F5C8A9A2C611320181ADED7A50690A6E5875DC73E5977C7FE64AD5
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.$..PE..d.....f....."....."....(.....x.....@.....`.....a..x.....P.....0E...@...).....Z..8.....pY..(....A..@.....`f.....text....&.....(..... ..`.rdata..\....@.....,.....@..@.data.....@....pdata..0E.....F.....@..@.00cfg..8.....@..@.gxfg...p$... ...&.....@..@.retplne.....P.....(.....tls.....1....`.....*.....@..._RDATA..\....p.....,.....@..@.rsrc...P.....@..@.reloc.....2.....@..B.....

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2304416
Entropy (8bit):	6.440570911194646
Encrypted:	false

SSDEEP:	49152:bCbc+v3neoFjYL1yOWK6NAxq8N0+cP27KIE:0v21yyxhl/
MD5:	D737A64C835D918DBE53B2C7724488FF
SHA1:	E5C7003AB10328E95D015AA75C08479B4CC1005F
SHA-256:	E8ACDD3FDF21ACE7F2A5A1A82CE5655A18FC52FC81D354A5FF685AA868FE1A98
SHA-512:	D6E90B9B32B2C5D3FEB0012E3A5BE5AA6E27801FECDE87BEF64D7BB8A23FC5BBDDE2A60A42F001B7515188B8BF23F8C959308C465F88FB62798814611021BAAA
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.$..PE..d.....f....."..... .....@..... .....$.....x*#...`..... .....`...b.....h.....". ....P!.....#..)....$.H.....8.....(....S..@.....(..x..... .....text...,..... ..`.rdata..0....@.....2..... @..@.data....A.....@....pdata.....P!.....@..@.00cfg..0....@"..... .....@..@.gxfg..../...P"..0.... .....@..@.retplne....."..... .....tls....."..... .....@...LZMADEC....."..... ..... ..`_RDATA..\....."....!.....@..@malloc_h....."....!..... ..`.rsrc... ....."....!.....@..@.reloc..H.....$....."..... @..B.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe.1711737406.old (copy)

Process:	C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2304416
Entropy (8bit):	6.440570911194646
Encrypted:	false
SSDEEP:	49152:bCbc+v3neoFjYL1yOWK6NAxq8N0+cP27KIE:0v21yyxhl/
MD5:	D737A64C835D918DBE53B2C7724488FF
SHA1:	E5C7003AB10328E95D015AA75C08479B4CC1005F
SHA-256:	E8ACDD3FDF21ACE7F2A5A1A82CE5655A18FC52FC81D354A5FF685AA868FE1A98
SHA-512:	D6E90B9B32B2C5D3FEB0012E3A5BE5AA6E27801FECDE87BEF64D7BB8A23FC5BBDDE2A60A42F001B7515188B8BF23F8C959308C465F88FB62798814611021BAAA
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.$..PE..d.....f....."..... .....@..... .....$.....x*#...`..... .....`...b.....h.....". ....P!.....#..)....$.H.....8.....(....S..@.....(..x..... .....text...,..... ..`.rdata..0....@.....2..... @..@.data....A.....@....pdata.....P!.....@..@.00cfg..0....@"..... .....@..@.gxfg..../...P"..0.... .....@..@.retplne....."..... .....tls....."..... .....@...LZMADEC....."..... ..... ..`_RDATA..\....."....!.....@..@malloc_h....."....!..... ..`.rsrc... ....."....!.....@..@.reloc..H.....$....."..... @..B.....

C:\Users\user\AppData\Local\Programs\Opera GX\launcher.visualelementsmanifest.xml

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	4.996593526126476
Encrypted:	false
SSDEEP:	6:ejHyaVic4subiL/bWHMjizddDhkQwYZXXKmJfFmkQwYEbghuPYEpwhugVFQ:eF8iDbWHMjizd2O/fbrghuP5whuQFQ
MD5:	E8D8EAA4C2826C083AB9243B5CBD7BF8
SHA1:	534361AE03417DFD14EBD6F961B707C75A2AF41A
SHA-256:	B3213B07F691C812425115428B9D6E0637D488159E0A1C160C8FA8F04DED11F6
SHA-512:	8ECCD5EF54A73E915A39CDEF9768837DD16E49AE27A3AE6428FB346C9C838FD9DBEDC3F40A9094754C770CA2236A0D2DFDE37D22289218D862AF5E8BC15E8E5
Malicious:	false
Reputation:	unknown
Preview:	<Application xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">. <VisualElements. BackgroundColor="#06030D". ShowNameOnSquare150x 150Logo="on". ForegroundText="light". Square150x150Logo="Assets\150x150Logo.png". Square70x70Logo="Assets\70x70Logo.png". />.</Appli cation>

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

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	480672

Entropy (8bit):	6.407077061099877
Encrypted:	false
SSDEEP:	6144:7AIY0X8PU5lauzzHfkgJvPAFrmFNVcPif2csfraP3qHH:7AIhsPUjauzzHfNVFNVcPO2cq+P3qHH
MD5:	F4CD4AC3B97BFECC0B1B204BB02A6D44
SHA1:	246FDEB112A0CD651C23D455232EB7F8D31ED41D
SHA-256:	42089A9C43D4715413A971F3E9B0F01B718A5FC7DC220A87608297635E2758D2
SHA-512:	3574CC3C24BEC63523D5B70158AFFFF720C40E9E62266F113A69B4C11AC9308F27B6A87D39555C0AB546111019667936D54AADF929C55EA225DB7A28A260A8A
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.$..PE..d.....f....." .....$.....6`....`A.... .....h...x...(.....H.....A...,...).....H.....8.....(...@!..@.....!.....text...z..... ..`.rdata..... ..... @..@.data....K..... .....@....pdata...A.....B.....@..@.00cfg..8....@.....@..@.gxfg... &...P...(.....@..@.retplne.....tls.. ..!.....@..._RDATA..\.....@..@.rsrc...H.....@..@.reloc..H.....@..B..... .....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\libGLESv2.dll

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7640992
Entropy (8bit):	6.489540842464174
Encrypted:	false
SSDEEP:	98304:r/5OeM37DfzKVyOzyWblxFz4t/BpTSE+b6rlTDYP1TSU3Xm3y4t1FDe:r/1MLzmVNzB6rZG1TVCy4t1F6
MD5:	0948651B610250144369FB114E0A1597
SHA1:	662165F38925C712024D36847FAFC55F705E9C8A
SHA-256:	D98F9E4FA6DEE9EA08E8760C594600E280C5A7AF5E552BA65446081FBBCD4966
SHA-512:	5DAE8D0C597FDA5D62F2D2A3437EFFCE415457EFD9DB3D842ADC4AEB3BFE08D48151F14AECE25D81824268BDCFAA0069A4A74F5319393D49624060C13831E 91
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....." .....Y..T.....P}F.....pu.....^ u...`A.....k.....l.d.....t.....q..Y...nt..)....t.....\vk.8.....0uk.(....1Y.@.....l.....k.@.....text.....Y.....Y..... ..`.rdata...]...0Y. .^....Y.....@..@.data.....m.....vm.....@....pdata...Y....q..Z....q.....@..@.00cfg..8....t.....`s.....@..@.gxfg....,... t.....bs.....@..@.retplne.....Pt.....s... .....tls....B....`t.....s.....@..._RDATA..\....pt.....s.....@..@.rsrc.....t.....s.....@..@.reloc.....t.....s.....@..B..... .....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\bg.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	809086
Entropy (8bit):	4.792072887577772
Encrypted:	false
SSDEEP:	24576:JOEtuS31gRhcQ7E6N/fhIhIK6g2HK2JwZLvY2zQkECEUiVbMqquIWKVDVLts37Nz:JOpSs7xAI5K2JwZLvYT9UiVbbqxKVDV8
MD5:	069435B6240FD89EBDC05353CEFE1ADF
SHA1:	62CACFD36CC03F692E37BDB285873D02653C5020
SHA-256:	09A3501A3332D4609353C57C23F8A27BB1A215A9E07B52BC65E819C261DD6CDB
SHA-512:	D65C8439D88440A85D5FC78581B506A7461DFBD0463F8538870C016FFD90C3D4A728E6666CD05BF72363B45647065783CC10CD3BBDE0DEC3EE63F89DD2E019
Malicious:	false
Reputation:	unknown
Preview:	.....y%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.2...w.?...y.E...z.T...|.Z...}.l.....t.....y.....,..... ....W.....b.....j.....|.....*.....2.....z.....d.....).....X.....U.....h.....A..... .....$.....Q.....^.....A.....i.....K ....t!.....!....H"....g".....".....z#.....#.....#....s$....$..../%....U%.....%.....&.....&.....'....'.....(.....).....)....e*.....*.... 3+....c+.....+....k,.....,.....,.....-...../.....0.....0....<1.....1....X2.....2.....3....M3.....4.....4.....5....D5....26.....6....G7....|7....l8....G9.....9.....:.....;.....;....C<.....<....X=.....=....K>.. ...>....'?.....?.....?....#@.....A.....A

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\bn.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data

Category:	dropped
Size (bytes):	1039857
Entropy (8bit):	4.3831224078899185
Encrypted:	false
SSDEEP:	3072:kbt+7m0FhX/ShdYH1/RFb/sHFe1XCqoEgFM:o+7pWghbyFK9dF
MD5:	EA60EE4E0F963ACEB074A516B2D6ADFB
SHA1:	7B053259B20E300ED7DA840C50742DEFE3123193
SHA-256:	65916DEDD8DF9C32471C2FBDFD368F4EA4AD6FA69CB7DF129BCA130481793DBD
SHA-512:	F9683D4C4CC33D9EB2DD2101DD547A405AB8B62448D0C950E9578F3677248D3303C232948EA25341A0AE7DCA86C2E20AC5B2194A97E93D1BAC07BB67FCAA1E 25
Malicious:	false
Reputation:	unknown
Preview:	.....%..e.....g.....h.....i.....j.....k.....l.*...n.2...o.8...p.E...q.K...r.W...s.h...t.q...v.....w.....y.....z.....|.....}.....+....`..... .....l.....d.....2..... ....X.....5....\....:.....&.....h.....:.....O....J.....4....."..... .....u..... ....&!....j!....!...%".....".....".....#.....#.....$.....%....D%.....&.....&.....&....*'.....'.....(.....(.....(.....)....C*.....*.....*....b+.....,....V,....|,.....-...../...../.....0.... .1.....2....[2.....2....}3.....3.....3.....4....s5.....5.....6.....6.....7....h8.....8.....9....-:....y:.....:.....;....?<.....<.....<.....=.....>....-?....f?.....@.....A.....B.....C....JD....LE.....E....VF....8G.....G.. ..aH.....H....gl.....J.....J.....J.....K

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ca.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	513027
Entropy (8bit):	5.432519176352726
Encrypted:	false
SSDEEP:	12288:JQFmiLH+7C6ybGbf1bCCrz+W58rmUUkcvKOl3nRWgZO5F5i3RoCQrGyTSHNBe935:yHJ/8atIRF1kJd0njPYX
MD5:	18326F23AA856DC640E52CF3118C9B8E
SHA1:	8546BBFB20FDB9D385724B838C6B5F2D320F615F
SHA-256:	ACD7EA2DC2A510147CF37405194FCB95113E0A51EF2EC962C2E428EE8E2B0115
SHA-512:	7F6689389423A850009199EBEBE364A0360D9A39FAAFEDC51F9D4BE7E75142F498536B4F585AD55BB655571875DC6BEB73D562A0CFCFEE443640832A99A5F3D
Malicious:	false
Reputation:	unknown
Preview:	.....q%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v."...w./...y.5...z.D...|.J...}.\.....d.....i.....q.....y.....F..... .....@.....{.....].....a.....X.....!.....{.....1.....W.....).....k.....9.....p.....b.....^. .....B.....h.....I.....e.....%.....5.....(.....-.....B.....*.....>.....h.....K.....k.....!.....=..... !.....@.....c.....,.....g.....+.....D..... .....5.....C....._.....= ....g ....6!....i!....!....!...""....J"....]".....".. ..5#....u#

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\cs.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	507732
Entropy (8bit):	5.86532539438707
Encrypted:	false
SSDEEP:	6144:IfAC3uuuNLX9rbVQnmVzYSUNOfs8SB08QJs+mLJ1XiLqvL4OQp:C/yBNrbVDVzYSUNOU8SVfC
MD5:	B41A26054D8E72602A9AB7C697678F96
SHA1:	8BCF77844B545F9AC8CED0D86F3F6B0416C5F5A2
SHA-256:	174AC36585B8F6C2C1822AEE05E1FB4EC73E984846D5DE29F2B849F7900EAB65
SHA-512:	18E6B530CFC63F4AABD29DBE0D69F71514673706A5E997A67E5EB3AA26AD482FB50B736F92BF8781A7C5951D64CAB89368DDD84B4054EB86AA8DC78BF72AB0 78
Malicious:	false
Reputation:	unknown
Preview:	.....%H.e.....g.....h.....i.....j.....k.....l.!...n.)...o.....p.;...q.A...r.M...s.^...t.g...v.|...w.....y.....z.....|.....}.....,.....A.....o..... .....M.....z.....R.....k.....P.....f.....U.....}.....e.....K.....<.....#.....\.....t.....G.....|.....|.....K. .....(....._.....@.....\/.....C.....>.....3.....K.....w.....:.....Q..... .....b.....h.....n.....#.....Z.....\/.....B.....W.....1.....r.....x.....V.....'.....H.....+ ....U ....j .... !....E!....Y!.. ...!....3"

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\da.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped

Size (bytes):	470889
Entropy (8bit):	5.495569110921885
Encrypted:	false
SSDEEP:	6144:t0boyL+ytCnoN90zVWilNMzPZJTd46RGw2wEzZhxqENiB3n47A7De+AHpsMclpHr:tfyLNHNCMzxR7SqENil/AKdTHr
MD5:	CBE27BAC580522BB951F8BBAFFBCAD3B
SHA1:	5668179351E705F10A24EF9464382BA6152C8B10
SHA-256:	9793C9F49DE1B1362C0DA4618BFFBDC5FACE9942E301A0B7FCF0E4E9E72D5535
SHA-512:	912408F1CD830E7BFF3AF1D7568FBC419DFC07A6FDFE15769632F7CCEBA7837380D71F6D84009C756044950005D050ADAA704B6925D2EC510E5874715798AA4
Malicious:	false
Reputation:	unknown
Preview:	.....T%..e.R...g.Z...h._....i.p...j.|...k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.....|.....}.+.....3.....8.....@.....H.....P.....W.....^.....e.....f.....g.....i.....w.....+..... .....`.....'.....3.....l....._.....G.....q.....H.....w.....}.....F.....m.....&...../..... .....,.....*.....g.....@.....+.....1.....*.....i.....R.....C..... .....'.....{.....X.....u.....m.....=.....=.....U.....Q.....(.....^.....Y.....3 ....O ....\ ....!

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\de.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	512947
Entropy (8bit):	5.526944497993563
Encrypted:	false
SSDEEP:	6144:SqDFDzwXNn6LeN5U2ztCaXdzlbBtCS94LlS5lmkVQAUDM:S+DzwjUWCatdCS91eRM
MD5:	9326997FFB3A1039FB8BFE9D66DE9917
SHA1:	EE70119DE4FB4C5385DA1D0F79CACB77D43CFBA2
SHA-256:	D8A2DDACEA96640CBC7144F662282DC2B0CF0A8B7DACE957BEE32C69D31830DE
SHA-512:	97E69AC95BF078647220935A76882728F9C9410513CBABFDAD3A2CB990C7B6C47DE62591A41A77048636DA8A070E5786AAC0B8044097A1C0255BA2A031F957F5
Malicious:	false
Reputation:	unknown
Preview:	.....$l.e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.(...v.=...w.J...y.P...z._...\|.e...}.w.....n. .....C.....;.....X.....-.....A.....G.....~.....0.....O.....`.....b.....l.....l..... .....m.....~.....*.....).....:.....G.....F.....o.....(.....R.....d.....j.....d..... .....b.....U.....V.....t.....p.....; ....}!.....".....U".....\_".....".....\|#.....#.....#.....X$.....$.....$.....%.....t%.....%.....&.....&.....&.....'

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\el.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	875935
Entropy (8bit):	4.880943970317316
Encrypted:	false
SSDEEP:	24576:2ykN6BN08fjsCKG9w+ZzD2xEEbvL7Ffrk+mIeJFlmfPPpqpWblzK0Yt2cd8ZKoMZ:2EBN08fjsCKG9w+ZzD7EbvL7Ffrk+mIL
MD5:	6F6CCD956162C7BC4C9A38AB6B036370
SHA1:	C7D3EA4F2C5DCE0169E01FDC90AF07B991BD76BE
SHA-256:	6C9BA5EBF7A1047858350D08FB108C6A47F413B97F716999C38AD04C50429667
SHA-512:	952BC5E564FA88F808A5FD9E13B38D82034E4C89C027E8AE1D39B9938B9846CA4FC576912F58E5574C2500D9FE84158C14AC70A50C49785C0A64DD463B22B4C
Malicious:	false
Reputation:	unknown
Preview:	.....B%$.e.....g.6...h.;...i.C...j.M...k.\...l.g...n.o...o.t...p.....q.....r.....s.....t.....v.....w.....y.....z.....\|.....}.....!.....(...../.....6.....7.....8.....:.....a.....8..... .....Y.....k.....l.....l.....~.....d.....*.....).....P.....X.....R.....!.....2.....M.....4.....b.....~.....9.....#. .....j.....?.....M.....; ....w ....R!....,"....".....".....#....X$....$....$....%....&....&....'....'....(.....(.....).....).....*.....*.....+.....,.....-.....-.....-...../.... ./.....0.....0....>1....w1.....1....P2.....2....>3....k3....X4.....5.....5.....5.....6....;7....w7.....7....i8....+9.....9.....9.....:....V;.....;.....<....9=....T>.....?....C?....D@....+A.....A.....A.....B.... .C....rD.....D....^E....(F.....F.....F.....G.....H

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\en-GB.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	414723
Entropy (8bit):	5.552932998647449
Encrypted:	false

SSDEEP:	6144:U0929nnBblkE8JSQr6BcGRgwCfDyv2QKus46d92WR2:U4Qw3JFrQGii46lR2
MD5:	99B9B49CAE689E3561C827EA02635F9D
SHA1:	2CAF079F32362D22D68BE858159F265409D18E32
SHA-256:	7063979166F0B1A0ABA5B4E090D702808BB62D9326A518BE86EA4BBB2E6E96A2
SHA-512:	73D74789E4CE260F0D5C370AB22F3ABC2804B60D4EE9E3FCF2BD85C761DAD135E08EFC4316583FB82A03821B3643139963806 53C4699192749063AD0EA259141
Malicious:	false
Reputation:	unknown
Preview:	.....%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.!...q.'...r.3...s.D...t.M...v.b...w.o...y.u...z.....|.....}.....7... ..J...../.....+.....A.....*.....v.....<.....J.....o.....=.....r.....+.....\.....j.....<.....r..... .....&.....e.....?.....^.....h.....n.....O....._.....G.....R.....t.....m..... ../.....k...../.....P....._.....8.....^.....b.....Q.....L.....s.....x.....B.....^.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\en-US.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	417185
Entropy (8bit):	5.550011130613742
Encrypted:	false
SSDEEP:	6144:uEI84cHEA33RyrZngn/OsiwYzSyvepwG326O9bUR2:uN8BpcrIiwSlC26PR2
MD5:	E41F1594692F65CF99502F40582C82D7
SHA1:	7787AE80BBC73CC16E8E8118838DE2A3971AF2AC
SHA-256:	4FD95212B6ECBDC1C58388148EA2314CE5EA5BCD11BDDF05E51B14404D2746A6
SHA-512:	80047E2312B48ECF68BD3A7AF1D38F23ACB390293F8B31656D5DE72F9DD71A574D17DAB3656B34DFD513673CC876E2BA464BDA58BF420D5D9B7E5B8F049077 5
Malicious:	false
Reputation:	unknown
Preview:	.....%..e.....g.....h.....i.....j.%...k.4...l.?...n.G...o.L...p.Y...q._...r.k...s.|...t.....v.....w.....y.....z.....|.....}.....".....4.....D.....U.....).....q... .....'.....X.....h.....'.....c.....y.....L.....a.....).....r.....:.....{.....j.....X.....Y.....i.....).....4..... ?.....S.....1.....l.....5.....A.....|.....G.....L.....t.....6.....A.....:.....O..... .._.....a.....6.....k.....(.....7.....u.....q.....-..... .....=.....a.....y.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\es-419.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	502335
Entropy (8bit):	5.40727042571361
Encrypted:	false
SSDEEP:	6144:Dd4SYg2R2cJwZCXizXu2ndN/Bm+LJgwbYf+cwdyEcG2Bj1B3F9iBHKvI4:54SYgg5izuINx3cwdyzYqvd
MD5:	2966795E0B931BADB32374A6244B7868
SHA1:	7744C5801BAEC1B76EDE8A9429CA35C6E3BF55FE
SHA-256:	720014CD29A97B1C911DD887BC69D3833178211C882E72109FDF391CC6C2C499
SHA-512:	85D263AC49D7E3280CE14C9E614A10AB666F5BA3AE8EAAEB1228356DDA11D38A5A84A7CC30272D5A9012E305A797F4BBCE987D72AF4E811A072F30C90EB92E EE
Malicious:	false
Reputation:	unknown
Preview:	.....v%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.-...w.:...y.@...z.O...|.U...}.g.....o.....t.....|..... .....r.....c.....@.....^.....K.....K.....u.....E.....m.....~.....x.....w.....+.....U.....2.....w....._.....2..... .....s.....1.....`.....{.....&.....T.....c.....%.....[.....q.....N.....j.....`.....E.....u.....M.....b. .....l.....S.....{.....2.....s.....".....H.....b.....#.....X.....q.....>.....3..... ....1 ....7!.....!.....!.....,".....".....".....>#.....#.....#.... .#....@$.....$.....$

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\es.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	498817
Entropy (8bit):	5.394334592286179
Encrypted:	false
SSDEEP:	6144:tkh0VbOA9k8812cjsjiHa/HJTP6PZOk8jOwgcXg1+y183yOY+KnTzP1X7jHUoEWh:tkh0VbOA9k8Li6/H3Dz683yp7jXXI9E
MD5:	7C3587F68CC1E3984A6604B26E746759

SHA1:	5DBCDC4804311429C2CE463CD9F59EA0810C38C3
SHA-256:	8F984030BCE1792A4C6AAA7813A12B25DE55018741EE0B4A8A684247B08C4753
SHA-512:	918CECAD97C3DBE3E6FF93E3132CEB94231F23C7694B6C5AD9B92E9D2C93B5067C9F006D0FEF791F63E53BD7EC2C73EC4B37C6A057520CAEE486EC9FF653A5C6
Malicious:	false
Reputation:	unknown
Preview:	.....j%..e.~...g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.!...y.'...z.6...|.<...}.N.....V.....[.....c.....k.....s.....z.....w.....o... .....l.....X.....H.....b.....E.....W.....X.....8.....V.....q.....R.....".....S.....x.....-.....`.....v.....".....J.....Y.....R.....h.....4.....g.....z...../.....c.....o.....M.....X.....0.....:.....'.....7.....%.....l.....<..... h.....6.....]...../.....c.....#.....u.....i..... .....:.....N.....Q ....!....E!.....!....("....i"....}"....."...."#....H#....[#.. ...#....,$

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\fi.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	467188
Entropy (8bit):	5.475064085956737
Encrypted:	false
SSDEEP:	12288:RV1s819a+fl/2BEqWaVufYfZhuQ/bOYd2YlVtcKXrGkc1JQ:ly2GmrEIr
MD5:	A9ACAB0B24DFACE9A64E78369836F851
SHA1:	FF2A3BF13F3F79056591D557CC229E0F3F2FFE5E
SHA-256:	5658D14A4754922E98CBC9017FB90E013CE9B1FF2EB87C58419ED3E98AA00178
SHA-512:	B509174CF0C7D9AA74778CC529B48D1B2512F553E680180A22036150436238EB8D01243ED3D7165F8159DC107984F3C8788B44815E5E68E0170CB2FEF150BA74
Malicious:	false
Reputation:	unknown
Preview:	.....%Y.e.....g.....h.....i.....j.....k.....l.....n.....o.....p."...q.(...r.4...s.E...t.N...v.c...w.p...y.v...z.....|.....}...../.....4..... .....b.....>.....H.....&.....o.....K.....q.....n.....(.....|.....$.....~.....'.....G. .....p.....J.....Z.....{.....*.....T.....^.....=.....J.....w.....[.....P.....m..... .....:.....0.....8.....x.....U.....M.....&.....t.....!....._.....&.....~.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\fil.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	521436
Entropy (8bit):	5.300414613948606
Encrypted:	false
SSDEEP:	6144:o8xZxWpc9B4FqwCGUoufaPNDtnJsy5WBE2bKUfm4:oNLIoTHWBlKL4
MD5:	FCBA6E51F1608B1F8C20A53228F7A0E3
SHA1:	E6A96AACD82B9559FD1895F3FB436CC1FA9E68D8
SHA-256:	6190A1353D3B59A3954082AD42CCEDF474D9493A816E4C33C7BF70357C266822
SHA-512:	835F3E462C6A200BE54AEFC7E2A09ABB218F1411C376E3390C49A5A64B3EDB99AB503C8C845F4EE7556FA3E78375AC6CC4D194C1D44A1B9F9A007CE7675F2750
Malicious:	false
Reputation:	unknown
Preview:	.....%..e.^...g.f...h.k...i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.$...\|.*...}.<.....D.....I.....Q.....Y.....a.....h.....o.....v.....w.....x.....}.....r..... .....a.....v.....x.....e.....?.....L.....@.....o.....t.....2.....H.....2.....o..... .....}.....i.....J.....u.....@.....h.....u.....).....S.....b.....?.....z.....\.....d.....e.....g.....$.....y. .....$.....s.....c.....E.....\|.....C.....m.....e.....A ....!.....!....L"....."....."....[#.....#....*$....[$.....$...;%....q%.....%.....% ....A&....i&.....&.....&....u'

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\fr.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	533204
Entropy (8bit):	5.42656536496862
Encrypted:	false
SSDEEP:	12288:bTlsXvu432L72zNvxcgw1IaSVATiwsn8Zw4rMYnYbGBA3z8GABqXJRCxB2gTSWeI:bTO0N1GAMf
MD5:	299FDEC5C529F686A75CA8DD249C28DB
SHA1:	BFBE364AF58B9C4A967F5A8CE826DA5EB2AF6AD9
SHA-256:	78C7BB9624B063607896C34122469F849BD49C24962863BB31CF1D971D885050

SHA-512:	BD34415842DF72127CDC05ABE58F9C73CD90F5C2C5AF0AF32B514066FD32F0A57DA05E01DA8A531E36F28F3E164BAB945D96CF7592489630051474F17C2A394
Malicious:	false
Reputation:	unknown
Preview:	.....h%..e.z...g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.&...y.,...z.;...|.A...}.S....[....`....h.....p.....x.....x..... .....,.....n.....e.....7.....<.....\.....G.....D.....z.....2.....K..... ....o.....M.....N.....H.....`.....y.....(.....|.....i.....b.....q.....N.....|..... .....2.....R.....p.....9.....v.....*..... ....y.....y.....#.....?.....+.....x..... ....!.....!...5"...\"....."....g#.....#.....#....($....\|$....$.....$.. ..;%.....%

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\hi.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	1067175
Entropy (8bit):	4.410832963989589
Encrypted:	false
SSDEEP:	3072:3UtowpoUCbp2+NpqOV/BB0ZV1d1EGZDS7WexEWUt2bhtWi2V8nC5kbLAbqmbeget:WoHUCHkwsLlqdd
MD5:	9907AB6C963DB1613E3811104F3DDD9C
SHA1:	549D59E22ABF5D80B5690EFE85B27438ACAA5A00
SHA-256:	0A485C447311495D55B8EAC8D4F00356A0250F95B44FD8C549DE59357084AA11
SHA-512:	9AA2986CA627158B6ECD23D65166D2E8B5B5E23DA8103FD27DB6C4212B61610BF73FD94CB68F028280D045CA78B4BF131CEFBC23BEE23FB2ABD911032E7E3F 4A
Malicious:	false
Reputation:	unknown
Preview:	.....{%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.!...t.*...v.?...w.L...y.R...z.a...|.g...}.y...../.....h.....L... .....j...../.....]...../.....l.....B.....#.....S.....).....P.....u.....Y.....D.....+.....Y.....x.....C..... .....@.....T.....Z.....> ....B!....m!....."....."....."....."....#.....$.....$.... %.....%.....&.....&.....'....'....o(.....(.....(.....)..../*.....*.....*....W+.....,....i,.....-.....-...../....l/.....0 .....0.....0....)1.....1....E2....x2.....2....]3.....3.....4.....4.....5....N6.....6....(7.....7....n8.....8.....8.....9.....:....H;....z;....}<.....=.....=.....>....e?.....@.....A.....A.....B.....C.....D....ZD.....E.... wF.....G....aG....UH.....I.....I.....I.....J.....K

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\hr.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	497570
Entropy (8bit):	5.5613731809737335
Encrypted:	false
SSDEEP:	3072:E/ryT/5LWXUGXkAPKRpjqlGaBV08LQFvBAGC7ZqVwcsRqH7c2Dn3LWO6AHshClBY:qw/5LU7X8Rp+ALqwAjSihswJKaSyCiZw
MD5:	09431A45311A97E2B598A26741AC3BC6
SHA1:	96D26E3D9217028A5A6900B1EF51E354442FEEE7
SHA-256:	E04D8A13FBC1B372D7C1FAD6F7A47BFC3CB4FB768B7BE66B1CD52191DBBECA76
SHA-512:	8ECACA63D58BC1849948DBC5A2833CFE605E9F36A47E5AD5CECED3AC040A9400156829CD13619A11B14AED4FE5237CE021F935FABEDBE669A0A5204697FA1 195
Malicious:	false
Reputation:	unknown
Preview:	.....%..e.....g.....h.....i.....j.....k.....l.....n.....o.#...p.0...q.6...r.B...s.S...t.\...v.q...w.~...y.....z.....|.....}.....".....N..... .....;.....n.....M.....!....]....s.....-.....-.....o.....=.....M.....R....w.....t.....O.....v.....!.....W....r..... .....p.....N.....`.....T.....O.....}.....W.....L.....w.....2.....-.....o.....-.....e..... .....K....j.....3.....`....w.....V.....).....x.....$.....R.....'.....y.....D ....2!....{!....!....!.. ..."....."

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\hu.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	531019
Entropy (8bit):	5.672617115733098
Encrypted:	false
SSDEEP:	6144:YWkE356hC5WRIHGDHbtGSmeFkQ9XmBdpEN/3ICEqPHyNwkatTD5HvGTZfp6GcMAG:YWkcWL4ckaUsD5HvGys+4f
MD5:	06C8057DF87662E4AF3B693A88D04A9F
SHA1:	C2C1ECD1CF9AB7A1C5F56096F915B052684712AD
SHA-256:	A73FE543AE2EA5EA42CBF357EA58184E78FF561C29F61B4F52FB17C7B7D5F185

SHA-512:	161C8101D3FF8FA39F877E2752E3B5BD9DB6FF4200ECB5A1C45CEDBB6BFD014BF93B8593BF678BD3D0E8BF67DBB943B880F8528F5B690A82BB55FC0D79A321 02
Malicious:	false
Reputation:	unknown
Preview:	....."%D.e.....g.....h.....i.....j.....k.%...l.0...n.8...o.=...p.J...q.P...r.\...s.m...t.v...v.....w.....y.....z.....|.....}.....C.....W..... .....&.....D.....;.....E.....^.....8....._.....p.....F.....,.....6.....$.....X.....$.....'.....m... .....'.....G.....d.....<.....c.....{.....S.....~.....".....b.....x.....:.....#.....e.....y.....Z. .....6.....<.....T.....P.....<.....2 ...._!.....!....."....5".....".....c#.....#.....#.....$.....%.....Y%.....%.....$&.....&.....&.....'....o' .....'.....(....."(.....(.....)

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\id.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	450780
Entropy (8bit):	5.4223529482397606
Encrypted:	false
SSDEEP:	6144:A+gAIJgCRdcpJwkK563SzTHEjSEnmFBEiuUTn:A+sgqcpsEHnmFWUT
MD5:	AADFC73804D0AF347FF2406F8EA17327
SHA1:	BDCBD96015311F636FA4A1883AE9F7745F7C642D
SHA-256:	30ED0454488349AAE35E2023F6E04CBFBAD39DCCC9149C54FA8BD4C5C5058486
SHA-512:	F578EB1C6C20A9FDC302F36F2154ADA3DE28E065E3936E985CE28563D5B2C67E91AA46607A919AA06D983302B6C816401357339655415C7F350295B3BD1EE970
Malicious:	false
Reputation:	unknown
Preview:	.....c%..e.p...g.x...h.}...i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y."...z.1...|.7...}.I.....Q.....V.....^.....f.....n.....u.....|.....D..... .....d.....U.....q.....t.....R.....<.....D.....8.....c.....c.....%. .....,.....i.....(.....M.....Y.....%.....g.....B.....i.....P.....C.....y..... ,.....=.....f.....G.....+.....g.....A.....o.....~.....:.....v.....].....p.....F..... .....u.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\it.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	499094
Entropy (8bit):	5.328817560077638
Encrypted:	false
SSDEEP:	6144:15N/m7eMRmzh8YYQDLIefGgAFK54qG0e3qqzKpwLIBy5kxAjNuRtEmYS9lcZujgP:15N/2Ri8wRwLCZGd8JadT+
MD5:	158CCD4881619B7E465794335BC15ED9
SHA1:	8C17B1064BD34E6CA82CB5753ED24316E6C73EF5
SHA-256:	08DB2F75AB5815EF2CB54F27E75C507B0FDAB8089E59441ED0BFEE43EB3AC2E6
SHA-512:	851AB3B7D3B259FFAD9D30B65B1227E79B95662CB34E8D1CD6B5960D1665F456C78265D952C94B929008FBEE5D26E065B5CB04A2E1B2404BCB8FBF677188061 A
Malicious:	false
Reputation:	unknown
Preview:	.....W%..e.X...g.`...h.e...i.v...j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.....|.....}.1.....9.....>.....F.....N.....V.....].....d.....k.....l.....m.....o.....W..... .....E.....a.....&.....h.....y.....q.....5.....^.....+.....}.....D.....<.....&.....G.....d..... ..&..... .....u.....A.....m.....%.....O.....]..... ....*.....<.....#.....r.....F.....p.....(.....T. .....#.....X.....n.....2.....^.....s.....O.....1.....t.....J.....u.....m.....u.....e.....|.....v.....m.....% ...; ....j!.....!

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ja.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	599830
Entropy (8bit):	5.8281706210617825
Encrypted:	false
SSDEEP:	3072:32dINrcpX83p2UKGTuLuGrL13dAxXFlGxgK0usjSy+QUJNt4DYKVS7b0X7HZBFBV:3l2BjUFTq/flVqeVQdljYYNau34
MD5:	1B5D982CFC66F02F8AF503780ACA5176
SHA1:	B064393D8B059F5DAA48161DB720756F464C5AD1
SHA-256:	F4E00BC9855771706065E837D8085DDF52BCD47488A189209A7547D14DF40EDA
SHA-512:	A19A1C706D1B159B7904F7DA454FAF6F0B4A6D13210F52BACEAD7AFF17280B9FE7C23A168AACA32A869C52819BF5921182010878AA3F90A226F28F3A7767719

Malicious:	false
Reputation:	unknown
Preview:	.....$..e.....g.....h.#...i.....j.7...k.H...I.Q...m.Y...o.n...p.{...q.....v.....w.....y.....z.....\|.....}..... .....".....'.....@.....j.....F.....$.....B... .....8.....u.....(.....&.....3.....#.....T.....f.....4.....a.....q.....m.....[.....@..... .....S.....c.....>.....o.....~....._..... ..N.....P.....k...../.....Q.....m.....n.....\.....$.....E.....{.....M.....\.....X.....".....k.....7.....L..... .....3.....U.....:.....I.....y.....E.....7 ....Y ....h ....m!.....!.....!....B".....".....".....#....4$.....$.....$....I%.....%.....&....8&.....&....L'.....'.....'....2(.....(.....(.....(.....).....*....O*

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ko.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	501964
Entropy (8bit):	6.169334467010321
Encrypted:	false
SSDEEP:	12288:lINpoGuV39uqp7VKixMGLtlq7Hh1mrOerIi1HNGc36xKpVdKV2WBQL:lgpoGuV3WGm0l2z
MD5:	282C517076CBBC464595B5A04BCCDB14
SHA1:	51CED44010BFCFFB320B632CF27548855FAFAA02
SHA-256:	22489C861BCEF0D79A2FC03FB5A1C55E1176922FFBE89C05BC7C54C6C6F847B3
SHA-512:	424595BC00FFCCF77E8EE561634F14793CB8D539681BA6672EA224785C62010C8DBA798A2F4D2B721E9CB960D774591EF5C260BF0B74FF053AFC55F784F0A315
Malicious:	false
Reputation:	unknown
Preview:	.....$..e.....g.....h.....i.....j.....k.....l.....m.....o.....p.....q.!...r.-...s.>...t.G...y.\...z.k...\|.q...}.....V.....t.....M..... .....H.....f.....k.....z.....,.....@.....).....6.....&.....0.....@.....C..... .....Y.....}.....:.....\_.....o.....:.....J.....I.....L.....W.....Z.....X.....O.....?..... .....J.....d.....8.....T.....W.....j.....-.....:.....E.....\.....$.....S.....f.....9.....L.....=.....P.

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\lt.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	532287
Entropy (8bit):	5.6618162413155915
Encrypted:	false
SSDEEP:	6144:72fvn4ETX/XPIx7iGyyXaGcGYDj/T2lf6SxtCs1TsRaVKx52O:CfvJfldiGyjDj/76SxssmR/j2O
MD5:	587FEF1B576042E1D3918915FEC494B3
SHA1:	D957FFC8F7EBBB3245837E501A2CD790BA788569
SHA-256:	8D13CCA2F6BD9E51FDC7F919E41C9A4EA01C0BF78C780C1AD75BA0FBF47AA134
SHA-512:	E12AD4E4186321DF04EB6CF570094A5B5986C36027A44CF71738AA8467EE270DF8C9C77234D16102F6DCE286ECB52CBA0953EAB7E38ACEBDBD625E5F4187F1 2E
Malicious:	false
Reputation:	unknown
Preview:	.....^%..e.f...g.n...h.y...i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.-...|.3...}.E.....M.....R.....Z.....b.....j.....q.....x.....h.....V... ..q.....[.....u.....l.....6.....u.....1.....H.....B.....v.....%.....6.....G.....5.....o..... .....f.....f.....@.....y.....7.....J.....>.....x.....Q.....5.....C.....v.....Z..... .....+.....e....._.....O.....& ....H ....[..... .....!.....!.....!....u".....".....<#....`#.....#.....$.....$.....%.....%.....&....Z&....z&.....'.....'.....'.....(....\(.....(..... (.....(....|).....*

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\lv.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	530446
Entropy (8bit):	5.669799465505182
Encrypted:	false
SSDEEP:	6144:G4MYLxpFOV+yzyqU28c9ssRmK7Bp57YXQGBi5nbrNk8zptNctVFL8qRB5mhDssZm:TMy3OVPzr7f5XG8Nk8ai2x
MD5:	1E08EA238ABF7AAB7F23F1BAB5EE7F6C
SHA1:	D1C619187ABBF793BB10C6F8E275B098C65E37CE
SHA-256:	B59B19BA5920293FB0A8C6B5420904B47632E97A7A00FF8CF779EAC1783FB645
SHA-512:	595CBC15E7C694C5A17024B573E69F6297F170DC60BB4647D9D1F509247E32955BE90632896463FE02ED5041422EC43439657CD4C991F7D9BFDD982EB79FB23A
Malicious:	false
Reputation:	unknown

Preview:	.....%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.*...s.;...t.D...v.Y...w.f...y.l...z.{...|.....}.....0.....y. .....D.....W.....x.....l.....h.....G.....?.....U.....8.....O.....b.....t..... j.....V.....|....._.....m.....%.....y.....*.....<.....*.....a.....p.....Y.....r.....e.....}.....@.....[.....p... .....o.....%.....Z.....*.....d.....1 ....Q ....j ....n!.....!.....!....:".....".....#.....#....I$.....$.....$....j%.....%....%&....K&.....&....F'.....'.....'.....'....b(....}(.....(.. ..$).....)

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ms.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	465066
Entropy (8bit):	5.319654799734954
Encrypted:	false
SSDEEP:	6144:+1ZzO7mJZnRcE4ZzPtfcIQx89sQocTlqu:OZzC0nWE4hQxBW5/
MD5:	D38EA19CB1C529A5284F8C70E05601B2
SHA1:	54CAD7FA9CD399485056AD79A02AFCF90D25CB9B
SHA-256:	B2D6777CEA095DB001D5F8D861C6889DD9618B1365DA6CAC866DA82F514ACF4E
SHA-512:	8AFF259DE73A9440D61AD095CF6E842372606B047DD1A54B1B23D11463467D34F57C24C139DC1BAE096D6C98B9D4FCF5E6625DB20A08FCEA3A11298F338740A 8
Malicious:	false
Reputation:	unknown
Preview:	.....]%..e.d...g.l...h.q...i.y...j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.....|."...}.4.....<.....A.....l.....Q.....Y.....`.....g.....n.....o.....p.....u.....Y..... .....+.....G.....:.....J.....(.....i.....V.....^.....S.....X.....'.....H.....%.....y.....q..... .....0.....W.....l.....?.....f.....r.....9.....s.....A.....v.....7.....i.....s.....%.....U.....^.....K.....V.....9.....~..... .....:....._.....w.....>.....X..... .....1.....8.....M.....]..... W.....e.....4.....o.....A.....o.....|..... 3.....C.....

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\nb.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	455316
Entropy (8bit):	5.4739564830342475
Encrypted:	false
SSDEEP:	6144:2rl6DGqTc8jrGw6yyMrr+8f1SLqxs/Pryi6x1xljtCM:2rEDo8jrL6f8f1SmxMPnExljtCM
MD5:	B91F4826DC081EBC7791FB0837EF3A4F
SHA1:	7D00E2D5661E55A935236F52540ADC85DA433EF2
SHA-256:	3C787E535389FADD70ADB97E275A6C53850CCC09CBFEA15B8BB7EB9B35DF56F4
SHA-512:	698318CD1F911B4B44735BDA618CBF7010FE2ED32A69FEAE8D2636B46D72BFB6D3A4608D89D5AD93FC9C73A633A8887E7B35887CED65F8EA741B6AF98AAEF0 62
Malicious:	false
Reputation:	unknown
Preview:	.....Y%..e.\...g.d...h.i...i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.#...|.)...}.;.....C.....H.....P.....X.....`.....g.....n.....u.....v.....w.....y.....Z..... .....M.....b.....+.....d.....w.....W.....X.....F.....G.....s.....;.....H.....".....^.....#... ..=.....]..... h.....=.....b.....r..... .....E.....U.....T.....h.....(.....V.....f.....`.....p.....#.....L.....\.....H.....V.....@..... ....N.....t.....2.....Q.....j.....9.....K.....8.....w.....b.....n.....$.....u.....2.....E.....n.....6 ....b ....u ....!.... .!.....<!.....!....."

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\nl.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	468815
Entropy (8bit):	5.414013572567173
Encrypted:	false
SSDEEP:	6144:wge90JwO/GpXgcoQ6oTcRP65XDpIK4m/ucy:q0JwO/GpXgconoTcRS5TpIo/uB
MD5:	D2F3D7B4FA4AD57F773AE15EB3E70222
SHA1:	A1F217C981B38AC46CE18E4374374DE0FAB39997
SHA-256:	44E08FE6BF7F10DA6F94A81E7BB659A9238E5988E1907C34B999353FD07DAE21
SHA-512:	13B00CE1496BB2C1FB2CA26385FCCE612FF11BFA28FE8B59798DFBEEE9E60AFCFB59549BE0707C5C6FAC8BBBA1D97B1697C234CEA7A1E85EA74E0E93C367 7431
Malicious:	false
Reputation:	unknown

Preview:	.....m%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.#...w.0...y.6...z.E...|.K...}.].....e.....j.....r.....z.....r.....<... ..Q..... .....]....q.....X.....!....x.....\.....j.....:.....Q.....Z.....|...../....E.....9.... .....<....`....t.....3....A..... ...../.....I.....I.....6.....I.....k.....\..... .....?.....C....._.....A.....`.....m.....~.....I.....@.....7.....% ....}

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\pl.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	514993
Entropy (8bit):	5.7844368274597
Encrypted:	false
SSDEEP:	12288:AmtOK56Qa4eCQ08WoOBCEtfQfM6HCOb6/PQCUd79e3mFR/TYYdeMsucZr1iguIw:99lrJDMt
MD5:	AEAD81008645D092C0D4498C845D7A5B
SHA1:	A1B1CCF4250C20234C8D48A681666C77646FCA4A
SHA-256:	8D767C47DB1494BC90A7B98E98680DD60B246636275032E5EC00C119E9595F8E
SHA-512:	E0D5A15A57A08E70BA0181C95292920D740A6117E244C9BC7BD2160729A04E1DCD118A9D40CB23C4C95B442460EB0CE86C5E7DDE86F1A71CA1687DE7C2B67A 83
Malicious:	false
Reputation:	unknown
Preview:	.....[%..e.`...g.h...h.m...i.~...j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.....|.%...}.7.....?.....D.....L.....T.....\.....c.....j.....q.....r.....s.....u.....d..... ....._.....{.....l.....(.....u.....*.....0.....=.....c.....Y.....6.....L.....x.....<... ..X.....i.....E.....Q.....t.....8.....F.....H.....\.....J.....\.....B.....R.....).....9.....).....:.....$.....q..... ....#.....@.....W.....!.....G.....7.....L.....m.....7.....U.....I.....E.....a.....>..... .....3.....^..... ....E ....V ....!.....!.....!.....!

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\pt-BR.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	490961
Entropy (8bit):	5.462948787832137
Encrypted:	false
SSDEEP:	6144:NKT/ngth9TSzp8XR6BJv2cQ74WesRYcTzINBXBLTUpnDk/eds7:NigdXRosceesRRTy
MD5:	3BA421A36A38A2596C3EE23161D602BF
SHA1:	62D09596040F1B59AD0CB786A7B26166F4F57503
SHA-256:	23FFC508EF4C74DBECFD2EABFB74B48AEF082C51B0B436F83C7553EC4CECE580
SHA-512:	1E1E0616578D4BB4ACD4508B69784EA8E033A030A4EC4D4148D2603E7D27A9B953EE385AD9C128486C261BCA3124B780D4C6C08A03F7F55776C84CD28AD5964 D
Malicious:	false
Reputation:	unknown
Preview:	.....p%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.)...w.6...y.<...z.K...|.Q...}.c.....k.....p.....x.....x... .....[.....7.....#.....@.....?.....T.....$.....4.....,..... ....f.....f.....#.....(.....<.....*.....w.....". .....a.....A.....?.....B.....E.....'.....{.....U.....J.....L..... .....g.....>.....i.....z.....^.....d.....i.....=.....S.....T.....- ....{ ....!....S!....y!.....!....."....f"....."...."

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\pt-PT.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	496752
Entropy (8bit):	5.441144108166814
Encrypted:	false
SSDEEP:	6144:IsacpqKed3ar/HSSREbKdB4JVJJxhcXNa7o54Cm:EPKekrPSSREfR
MD5:	753B1B692756F0FE53B6DEDE8D1888CE
SHA1:	B094C3487235C313339E83F008F0B75FAC7765D6
SHA-256:	EF8114B2580AA4E7B521874314A41F2976F25B4C0386AD60913611111B5CB7AB
SHA-512:	8FBF6A429265817FFE1A986F761FF51A92949B780155ED206623292081AAB3B191DED036F47CAAE8A41009B62720B802179E52C3ECC84B802EADB66E53D08859
Malicious:	false
Reputation:	unknown

Preview:	.....%..e.....g.....h.....i.....j.....k.....l.....n.....o.!...p.....q.4...r.@...s.Q...t.Z...v.o...w.|...y.....z.....|.....}.....&.....8.....L..... .....*.....y.....Y.....t....._.....j.....K.....x.....x.....^.....6.....O.....\.....[.....k.....=..... .....i.....T.....L.....\.....d.....O.....(.....~.....l.....".....L..... ..$.....d.....~.....S.....s.....B.....#.....s.....m.....H.....`.....P.....5 ....D!.....!.....!.....!....7"....."

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ro.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	509817
Entropy (8bit):	5.49849407979343
Encrypted:	false
SSDEEP:	6144:EPdYjuEEcVjt7NgMs2bh61buj6rXEZK4N8AZqhYpGWKHCAuwooUL:ECyEBVhN1h6DrX3S8AEupG/HwJo2
MD5:	005A99E11F7476A646A3DC3BCCE7A584
SHA1:	2ABC00C2EE2A8BDC70110C582535C47AFD4B3F4A
SHA-256:	0E451350162A38118281FFF76BBDD3CD12A3B5A04EC8B3EAA259AFABF312E687
SHA-512:	B72DAFCC5183ADF310F36DA0A13AED24C88CED9227484DDDDA8CBEB851CDB1B0C2B53D547D178841AC8455A283109FE423C55594769A7DE49B2834C8ECDBA8D
Malicious:	false
Reputation:	unknown
Preview:	.....}%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.#...t.,...v.A...w.N...y.T...z.c...|.i...}.{.....p... .....K.....%.....:.....Z.....0.....<.....9.....j.....X.....5.....g.....~..... ....:..... ....J.....%.....l.....=.....b.....v.....;.....K.....6.....K.....-.....B..... .....p.....O.....j.....2.....L..... .....n.....m.....3.....s.....%....;.....R.....m.....1.....q.....x.....&.....N.....$ ....] ....u ....!.... 7!....M!.....!....3"

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\ru.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	812569
Entropy (8bit):	4.945155816034797
Encrypted:	false
SSDEEP:	12288:IGlU9XBlJfQjRo4YVepEaX+jhvYDfcwwgfhdxDkDtTKAYK2T5rqnjfRQjlvj3jDe:IGlUHlk56HII
MD5:	056C018007AD175D0CDF09C405309A20
SHA1:	DED584292EE8F9E468F9352BA75AD1FE6285A1A5
SHA-256:	F8FA2BA7A9FD9F64BA80C6CB3CDE2CCB72D3823081037AFA50CEAB9880F479BE
SHA-512:	78D38FD514BC7BFCC8D0A7FB109D2B9AA509FF05428DC2E09F6E2758EAE14BF0E69EA6CCA1F59DA85FEE099884A18897E235077CDEBF46F9CC4147ADC6243B5
Malicious:	false
Reputation:	unknown
Preview:	.....$\|.e.~...g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.*...y.0...z.?...\|.E...}.W.....\_.....d.....l.....t.....\|..... .....&... ..E.....6.....d.....r.....N.....+.....}.....#.....~.....p.....1.....}.....<.....i.....7..... .....\_.....0.....0.....O.....<.....m.....m.....o.....:.....X.....q..... ....N!.....!.....!....."....."....*#....N#.....#.....$....F$....a$.....$....|%.....%.....&....'....'....'....g(.....(....N)....v).....);*....*....*....2+.....+....o,.....,.....-.....-......./....4/....?0.....1.....1.....1.....2.....3....E3....d3.....3....]4.....4.....4.....5....:6

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\sk.pak

Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	515841
Entropy (8bit):	5.8288592928168645
Encrypted:	false
SSDEEP:	6144:Lf3JM+wEc0amAgCb7HBoh55fLwxdjJ6VcGyJXlk6BCle2cFBt4Ds:Lf3++dcD9FvHBozILwxd9seXlk6xvt4Y
MD5:	1C8221907D216D783B70D3C3C0A2D77A
SHA1:	D2DC893FC7109DC4560869BB6BD8CE9102FE279C
SHA-256:	5CF9F0D880DEEA644A6BADA0FCD46C8B695F5194A0D85AE06B6468F064080631
SHA-512:	9F03754615D5B47B732C797703B3B1EA43E8E35E2248AA251DFE7072A02C70198D2ABDCBF6F3E71A7C2F52BF6713D0E0B7E75F31FA50906FF3101018CDD1DD35
Malicious:	false
Reputation:	unknown

Preview:	.....t%..e.....g.....h.....i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.4...w.A...y.G...z.V...|.\...}.n.....v.....{.....R..... .....V.....%.....t....._.....~.....y.....5.....P.....s.....j.....0.....t.....E.....j..... .....8.....{.....R.....g.....x.....&.....9.....E.....X.....r.....'....u..... .....Y.....u.....T.....,.....n.....r.....?.....Y..... ....!.....!.....!....7"....X".....".....)#....X#....!#.....#.....$....=$....Q$.. ...$....H%

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\sr.pak	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	761766
Entropy (8bit):	4.890722517206804
Encrypted:	false
SSDEEP:	12288:dVvHT/9jexqeumgG37m8/k/nZ57LrXZasIfG+10B4snQgkCvCeeD74DMXWvAbvX:b93nbe
MD5:	0EC6F31A25588AD019FF0CCAD579E876
SHA1:	56768A15DD92532FD9EFECEBF106E567FD010A18
SHA-256:	6C784E3E3F95F970B3901B41F8114A411DBA3FEE6671F02AB5EC87502373895C
SHA-512:	1D37E60F41EB89E5FE5161207C98F1923C6637658001011B7F07990EFA3B9E4242EB34C0EA1074A7B7288DBFD64400B6DDE1D80AD91B6AF1AE0C69688FA59C7
Malicious:	false
Reputation:	unknown
Preview:	.....%..e.....g.....h.....i.....j.....k.....l.....n.&...o.+...p.8...q.>...r.J...s.[...t.d...v.y...w.....y.....z.....|.....}.....@.....e.....D..... .....a.....J.....~.....U.....o.....K.....&.....E.....H.....x.....g.....`.....-.....h.....?.....K. ....#.....8.....Z.....\_.....H.....q.....+.....y.....2 .... .... .....!.....!....3"....x".....".....?#.....#.....$....9$.....%.....%....0&....Z&.....& ....`'....'....'..._(.....(.....)....;)....)....*....*....*.....+....J,....,.....-.....-.....F.....s.....5/...../.....0....C0...."1.....1....#2....T2....A3.....4.....4.....4.....5....\6.....6.....7.....7....[8.....8.. ...8....Y9.....9.....:.....:.....:.....;

C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\localization\sv.pak	
Process:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
File Type:	data
Category:	dropped
Size (bytes):	460956
Entropy (8bit):	5.577281591773483
Encrypted:	false
SSDEEP:	6144:LyYzXk8Bn6V9l0p6zigMFlp4gfaVvZWtFi1cVKUI16wxg7mpO6Un/4i054nQUnBS:mYzVp6zt55W
MD5:	2B3638E67085D8280EC7ACB3E2F77AAA
SHA1:	925A502688A8235D6EE9F43E543E87E1EA9D466B
SHA-256:	CB98C2EE6C18D69310752F2223C626B445F80B1435C37247D26579DEB14E0292
SHA-512:	79B60208B4A80CFC4D2D47A9B8366397EC591A57215E95A5770D655D3CCABE17618165BB157B7F1D77B1F50DA67EC311EA3BD091241AAFE0375DAB1895C84B4 1
Malicious:	false
Reputation:	unknown
Preview:	.....`%..e.j...g.r...h.w...i.....j.....k.....l.....n.....o.....p.....q.....r.....s.....t.....v.....w.....y.....z.+...|.1...}.C.....K.....P.....X.....`.....h.....o.....v.....}.....~.....S..... ..4.....E.....V.....U.....*.....7.....7.....Q.....G.....g....."....P....._.....=....{..... .....q.....3.....R.....e.....9.....G.....'.....@.....)....8.....'.....w.....*.....?..... .....#.....p.....B.....:.....g.....V.....T.....o.....Q.....e.....Q.....~..... ....[....y ....E!

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:YBuZrEU8FTleUTKae2Kly029s4C1eH92
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 14:18:31 03/12/2024 13:05:00
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

Instruction
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 00007FCB60EC7115h
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 00007FCB60F69C07h
call 00007FCB60F6975Ah
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007FCB60EDCBB4h
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D84h
call 00007FCB60EC1D07h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [004C1D84h]
mov dl, 01h
mov eax, dword ptr [004238ECh]
call 00007FCB60EDDD37h
mov dword ptr [004C1D88h], eax
xor edx, edx
push ebp
push 004B654Ah
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007FCB60F69C8Fh
mov dword ptr [004C1D90h], eax
mov eax, dword ptr [004C1D90h]
cmp dword ptr [eax+0Ch], 01h
jne 00007FCB60F6FEAAh
mov eax, dword ptr [004C1D90h]
mov edx, 00000028h
call 00007FCB60EDE62Ch
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	

Name	Virtual Address	Virtual Size	Is in Section
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
.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

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
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
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

Name	Ordinal	Address
dbkFCallWrapperAddr	1	0x4be63c

Possible Origin

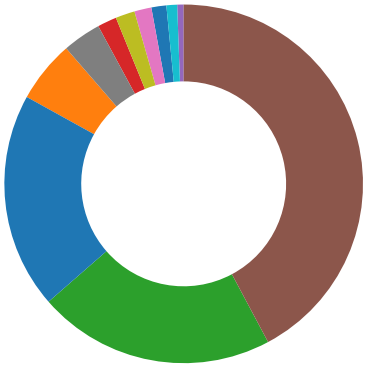
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

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

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Adware.Elemental.22.28512.27778.exe PID: **6960**, Parent PID: **2580**

General	
Target ID:	0
Start time:	19:35:14
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-6G7J7.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-6G7J7.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-6G7J7.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-6G7J7.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 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	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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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: **7004**, Parent PID: **6960**

General

Target ID:	1
Start time:	19:35:14
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-6G7J7.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-6G7J7.tmp\SecuriteInfo.com.Adware.Elemental.22.28512.27778.tmp" /SL5="$2040C,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-U02B5.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
C:\Users\user\AppData\Local\Temp\is-U02B5.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-U02B5.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-U02B5.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-U02B5.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-U02B5.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-U02B5.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-U02B5.tmp\is-CR25G.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-U02B5.tmp\CommonConfig_en.json	success or wait	5	60C4D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\is-U02B5.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-U02B5.tmp\is-CR25G.tmp	C:\Users\user\AppData\Local\Temp\is-U02B5.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-U02B5.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 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.$^l=\=\=\RichPE dR#	success or wait	1	4237AD	WriteFile
C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaLib.dll	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2f 3c fd fd 6b 5d fd fd 6b 5d fd fd 6b 5d fd fd 20 25 fd fd 66 5d fd fd 20 25 fd fd fd 5d fd fd 20 25 fd fd 7e 5d fd fd fd fd 58 fd 6f 5d fd fd fd 21 fd 7a 5d fd fd fd 26 fd 72 5d fd fd fd 20 fd 3a 5d fd fd 6b 5d fd fd fd 5d fd fd 20 25 fd fd 7a 5d fd fd fd fd 45 fd 2a 5d fd fd fd ec fd 6f 5d fd fd fd e5 fd 6a 5d fd fd fd fd 5a fd 6a 5d fd fd fd e7 fd 6a 5d fd	MZ@!L!This program cannot be run in DOS mode.$/<k]k]k] %f] %] %~]Xo]z]r]:]k]] %z]E*]o]j]Zj]j]	success or wait	8	5CC538	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-U02B5.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 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 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 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
C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\Config.json	0	25070	7b 00 0d 00 0a 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 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", "targetAppUrl":"https://try.opera.com/72TR8R7/KLRL579/?sub1=setupio	success or wait	1	5CC538	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-U02B5.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
C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\is-CR25G.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 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	737	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-U02B5.tmp\CommonConfig_en.json	0	17934	success or wait	1	5CC468	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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-U02B5.tmp\Config.json	0	25070	success or wait	1	5CC468	ReadFile
C:\Users\user\AppData\Local\Temp\is-U02B5.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: **5424**, Parent PID: **7004**

General

Target ID:	5
Start time:	19:35:50
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe" --silent --allusers=0
Imagebase:	0x1000000
File size:	3'581'600 bytes
MD5 hash:	1033B8A679409AAE694776CF2FDD3E8D
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_2403291835508755424.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1002E97	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	6B9ED0D4	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	6B9ED0D4	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	6B9ED0D4	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	6BA3E67B	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	6BA3E67B	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6BA3E67B	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	6BA552FA	CreateFileW
C:\Users\user\AppData\Local\Temp\5424_863545678	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BB41718	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	6B9ED0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.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	6BB4800F	CreateFileW
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	6B9ED0D4	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	6BB41C44	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B9ED0D4	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	6B99A447	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	6B99A447	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	6B99A447	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	6B99A447	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	6B99A447	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6B99A447	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	6B99A447	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	6B99A447	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	6B99A447	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	6B99A447	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	6B99A447	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	6B99A447	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\opera_package	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B99A58D	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\ded46497-8181-4fd6-9cf4-f6d96625d17f.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B9EBF4F	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\additional_file0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B99A58D	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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	6B9ED0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\additional_file1.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B99A58D	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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	6B9ED0D4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\files_list	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B9ED675	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\server_tracking_data	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B9ED675	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\ready	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B9ED675	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\pref_default_overrides	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B99A58D	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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	6BB41C44	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\1c35b91a-2459-41d7-b509-5957e986b2a9.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B9EBF4F	CreateFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\e556981b-ad85-4010-8d87-0f69b9322c75.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B9EBF4F	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	6B9EC3AF	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	success or wait	1	6B9EC3AF	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\assistant_installer.exe	success or wait	3	6B9EDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\mojo_core.dll	success or wait	1	6B9EDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\files_list	success or wait	1	6B9EDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\installer_prefs_include.json	success or wait	3	6B9EDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\opera_package	success or wait	2	6B9EDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\ready	success or wait	2	6B9EDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\resources\custom_partner_content.json	success or wait	1	6B9EDCFA	DeleteFileW
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835508755424.dll	success or wait	1	1001979	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5424_863545678	C:\Users\user\AppData\Local\Temp\.opera	success or wait	1	6BB41D33	MoveFileExW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\ded46497-8181-4fd6-9cf4-f6d96625d17f.tmp	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\installer_prefs_include.json	success or wait	1	6B9EC60F	MoveFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\additional_file0.tmp	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe	success or wait	1	6BB41D33	MoveFileExW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\additional_file1.tmp	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\resources\custom_partner_content.json	success or wait	1	6BB41D33	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835508755424.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 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	1002F54	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 38 fd fd 49 01 66 56 48 fd 1d fd 41 13 42 30 fd	sdPC8IfVHAB0	success or wait	1	6BA551DE	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 38 fd fd 49 01 66 56 48 fd 1d fd 41 13 42 30 fd	sdPC8IfVHAB0	success or wait	1	6BA551DE	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	0	105	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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	[0329/193551.250:INFO:installer_main.cc(453)] Opera GX installer starting - version 107.0.5045.79 Stable	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	105	148	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 73 2d 55 30 32 42 35 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	[0329/193551.250:INFO:installer_main.cc(456)] Command line: "C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe" --silent --allusers=0	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	253	58	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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	[0329/193551.250:INFO:installer_main.cc(478)] Uninstall:0	success or wait	1	6B9FD6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	311	55	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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	[0329/193551.250:INFO:installer_main.cc(479)] Silent:1	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	366	63	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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	[0329/193551.250:INFO:installer_main.cc(480)] Run Immediately0	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	429	55	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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	[0329/193551.250:INFO:installer_main.cc(482)] Backend0	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	484	62	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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	[0329/193551.250:INFO:installer_main.cc(483)] Inside package0	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	546	59	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 35 30 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	[0329/193551.250:INFO:installer_main.cc(484)] Autoupdate:0	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	605	67	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 36 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	[0329/193551.265:INFO:payload_manager_impl.cc(97)] Reading Payload	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	672	822	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 36 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 4f 44 64 6b 4e 6a 51 33 5a 57 46 68 5a 47 5a 68 4d 54 51 35 4f 54 67 35 4f 54 59 77 59 7a 67 78 59 6d 4a 6c 4d 6d 51 30 5a 6d 55 32 4e 44 63 78 4f 54 51 35 4f 47 56 6b 4e 7a 4d 79 59 32 59 7a 4d 7a 64 6c 4e 7a 68 6b 5a 47 4a 68 4f 57 56 69 4e 6d 49 33 4d 54 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	[0329/193551.265:INFO:installer_main.cc(610)] Tracking data: ODdkNjQ3ZWFhZGZhMTQ5OTg5OTYwYzgxYmJlMmQ0ZmU2NDcxOTQ5OGVkNzMyY2YzMzdlNzhkZGJhOWViNmI3MTp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOi	success or wait	1	6B9FD6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	1494	88	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 36 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	[0329/193551.265:INFO:settings_impl.cc(785)] Found 3 paths for standalone install mode.	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	1582	100	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 36 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	[0329/193551.265:INFO:resource_l10n_handler.cc(113)] Language not in the available languages list:	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	1682	103	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 32 36 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	[0329/193551.265:INFO:resource_l10n_handler.cc(119)] Trying language from system preferred list: en-GB	success or wait	1	6B9FD6C3	WriteFile
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 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 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	7	6BB41C44	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	1785	145	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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 6a 6f 6e 65 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	[0329/193551.672:INFO:scoped_download_folder.cc(59)] Installer download folder: C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	1930	113	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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 6a 6f 6e 65 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	[0329/193551.672:INFO:settings_impl.cc(1327)] Install folder set: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2043	59	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:settings_impl.cc(1382)] Operation: 1	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2102	66	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:wininet_impl.cc(755)] Stopping the download	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2168	89	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:package_fetch_sequencer_impl.cc(156)] Starting the package fetcher	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2257	99	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:package_metadata_retriever_impl.cc(333)] Preparing to fetch the download URL	success or wait	1	6B9FD6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2356	89	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:package_metadata_retriever_impl.cc(391)] Fetching the download URL	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2445	138	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:wininet_impl.cc(338)] Starting download from https://autoupdate.geo.opera.com/v5/netinstaller/gx/Stable/windows/x64	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2583	88	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:main_process_installer_runner_impl.cc(68)] Beginning installation	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2671	113	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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	[0329/193551.672:INFO:wininet_impl.cc(338)] Starting download from https://autoupdate.geo.opera.com/geolocation/	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	2784	1831	5b 30 33 32 39 2f 31 39 33 35 35 31 2e 36 37 32 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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 73 2d 55 30 32 42 35 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	[0329/193551.672:INFO:main_process_installer_runner_impl.cc(191)] launching installer backend: "C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe" --backend --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --cons	success or wait	1	6B9FD6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	4615	71	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 33 34 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	[0329/193552.234:INFO:wininet_impl.cc(611)] Initial request completion	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	4686	135	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 33 34 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	[0329/193552.234:INFO:wininet_impl.cc(635)] Could not get Content-Length from response: Error (0x13D) while retrieving error. (0x2F76)	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	4821	63	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 36 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	[0329/193552.265:INFO:wininet_impl.cc(885)] Download completed	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	4884	231	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 36 35 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 31 37 64 65 36 65 34 34 2d 63 64 35 32 2d 34 65 65 63 2d 39 62 31 36 2d 62 65 31 61 32 37 62 64 32 63 38 34 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	[0329/193552.265:INFO:wininet_impl.cc(338)] Starting download from https://features.opera-api2.com/api/v2/features?country=US&language=en-GB&uuid=17de6e44-cd52-4eec-9b16-be1a27bd2c84&product=gx&channel=Stable&version=107.0.5045.79	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5115	71	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 36 35 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	[0329/193552.265:INFO:wininet_impl.cc(611)] Initial request completion	success or wait	3	6B9FD6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5186	135	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 36 35 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	[0329/193552.265:INFO:wininet_impl.cc(635)] Could not get Content-Length from response: Error (0x13D) while retrieving error. (0x2F76)	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5321	63	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 36 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	[0329/193552.265:INFO:wininet_impl.cc(885)] Download completed	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5384	94	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 36 35 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	[0329/193552.265:INFO:package_metadata_retriever_impl.cc(485)] Fetching the additional config	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5478	224	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 32 36 35 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	[0329/193552.265: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	6B9FD6C3	WriteFile
unknown	unknown	99			invalid handle	1	6BB02B21	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5773	98	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 38 32 38 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	[0329/193552.828:ERROR:wininet_impl.cc(942)] Request completed with an unexpected HTTP status 404	success or wait	1	6B9FD6C3	WriteFile
unknown	unknown	62			invalid handle	1	6BB02B21	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5871	61	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 38 32 38 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	[0329/193552.828:ERROR:wininet_impl.cc(862)] Download failed	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	5932	92	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 38 32 38 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	[0329/193552.828:INFO:main_package_downloader_impl.cc(79)] Preparing to fetch the installer	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	6344	71	5b 30 33 32 39 2f 31 39 33 35 35 33 2e 32 35 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	[0329/193553.250:INFO:wininet_impl.cc(611)] Initial request completion	success or wait	1	6B9FD6C3	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\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	6B9992D3	InternetReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193551250.log	6415	63	5b 30 33 32 39 2f 31 39 33 35 35 33 2e 32 36 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	[0329/193553.265:INFO:wininet_impl.cc(885)] Download completed	success or wait	1	6B9FD6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZVZFKMB9\Opera_GX_107.0.5045.79_Autoupdate_x64[1].exe	0	1024	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$PEL'P(F-@@zbXy)	success or wait	49176	6B9992D3	InternetReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\opera_package	0	1024	4d 5a 60 00 01 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 52 65 71 75 69 72 65 20 57 69 6e 64 6f 77 73 0d 0a 24 50 45 00 00 4c 01 04 00 27 00 fd 50 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 08 00 00 28 01 00 00 46 00 00 00 00 00 00 fd 2d 01 00 00 10 00 00 00 40 01 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 0c 7a 08 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 fd 62 01 00 fd 00 00 00 00 fd 01 00 fd 06 00 00 00 00 00 00 00 00 00 00 58 fd 79 08 fd 29 00	MZ`@`!L!Require Windows$PEL'P(F-@@zbXy)	success or wait	49972	6B99A646	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	6BA55259	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	6BA55259	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	6BA55259	ReadFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	0	2048	pending	1	6B917EA4	ReadFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	0	2048	pending	241	6B917EA4	ReadFile
\pipe	0	1024	success or wait	1	6BB4046F	ReadFile
\pipe	0	1024	pipe broken	1	6BB4046F	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\installer_prefs_include.json	0	4096	success or wait	1	6BAFDF55	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\installer_prefs_include.json	0	4096	end of file	1	6BAFDF55	ReadFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	0	2048	success or wait	3	6B917EA4	ReadFile
\Device\Mailslot\opera_installer\C:\Users\user\AppData\Local\Programs\Opera GX	0	2048	pending	3	6B917EA4	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: **5172**, Parent PID: **5424**

General

Target ID:	6
Start time:	19:35:51
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\is-U02B5.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=0x2f4,0x2f8,0x2fc,0x2d0,0x300,0x6bc5623c,0x6bc56248,0x6bc56254
Imagebase:	0x1000000
File size:	3'581'600 bytes
MD5 hash:	1033B8A679409AAE694776CF2FDD3E8D
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_2403291835511345172.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1002E97	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	6B31E67B	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	6B31E67B	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	6B31E67B	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	6B31E9B7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835511345172.dll	success or wait	1	1001979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835511345172.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	1002F54	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\crashpad_5424_AXFIOWREYRVJSGNT	0	36	success or wait	2	6B335259	ReadFile
\pipe\crashpad_5424_AXFIOWREYRVJSGNT	0	36	success or wait	1	6B335259	ReadFile

Analysis Process: OperaGXSetup.exe PID: **5980**, Parent PID: **5424**

General

Target ID:	7
Start time:	19:35:51
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:	0x9e0000
File size:	3'581'600 bytes
MD5 hash:	1033B8A679409AAE694776CF2FDD3E8D
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_2403291835514565980.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	9E2E97	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835514565980.dll	success or wait	1	9E1979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835514565980.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	9E2F54	WriteFile

Analysis Process: OperaGXSetup.exe

PID: **3716**, Parent PID: **5424**

General

Target ID:	8
Start time:	19:35:51
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-U02B5.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=5424 --package-dir-prefix="C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_20240329193551" --session-guid=e8c1f83b-82a0-4cf5-8d29-c848e8638bca --server-tracking-blob=ZmUxNWFlNzQyYjk1NzA4ZTljODEyOGM4ZDY1NDg0M2YyNmVhN2MxNjg3MDQ5YmEyMGNjNzFjMzEyNjU5MGZjZTp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21lZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04NmE3YmY5NzI1Yjk0NDYxYjMzYzMzMGM3ZTA5NDUwMSZ1dG1fY29udGVudD0zNzQyX3NldHVwaW8iLCJzeXN0ZW0iOnsicGxhdGZvcm0iOnsiYXJjaCI6Ing4Nl82NCIsIm9wc3lzIjoiV2luZG93cyIsIm9wc3lzLXZlcnNpb24iOiIxMCIsInBhY2thZ2UiOiJFWEUifX0sInRpbWVzdGFtcCI6IjE3MTE3MzczMjMuMDMxNCIsInVzZXJhZ2VudCI6Iklubm8gU2V0dXAgNi4yLjIiLCJ1dG0iOnsiY2FtcGFpZ24iOiJQV05fVVNfUEI0XzM3NDIiLCJjb250ZW50IjoiMzc0Ml9zZXR1cGlvIiwiaWQiOiI4NmE3YmY5NzI1Yjk0NDYxYjMzYzMzMGM3ZTA5NDUwMSIsIm1lZGl1bSI6InBhIiwic291cmNlIjoiUFdOZ2FtZXMifSwidXVpZCI6ImU1ZWJhZDA2LTcxY2MtNDg4Ny1hOGRmLTdlYTdjNzkwMzhhYSJ9 --silent --desktopshortcut=1 --wait-for-package --initial-proc-handle=9C05000000000000
Imagebase:	0x1000000
File size:	3'581'600 bytes
MD5 hash:	1033B8A679409AAE694776CF2FDD3E8D
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_2403291835517673716.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1002E97	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	6ADAE67B	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	6ADAE67B	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	6ADAE67B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.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	6AEB800F	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	6AD5D0D4	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	6AD5D0D4	CreateDirectoryW
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	6AD5D0D4	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	6AD5D0D4	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	6AD5D0D4	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	6AD5D0D4	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	6AD5D0D4	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	6AD5D0D4	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\cb3aa22f-8954-4c6a-8828-0b23d4eea54f.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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-Light.ttf	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5BF4F	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	6AD5C3AF	DeleteFileW
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835517673716.dll	success or wait	1	1001979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835517673716.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	1002F54	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 38 fd fd 49 01 66 56 48 fd 1d fd 41 13 42 30 fd	sdPC8IfVHAB0	success or wait	1	6ADC51DE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	0	105	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 32 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	[0329/193552.126:INFO:installer_main.cc(453)] Opera GX installer starting - version 107.0.5045.79 Stable	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	105	1796	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 32 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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 73 2d 55 30 32 42 35 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 2d	[0329/193552.126:INFO:installer_main.cc(456)] Command line: "C:\Users\user\AppData\Local\Temp\is-U02B5.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	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	1901	127	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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 6a 6f 6e 65 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	[0329/193552.142:INFO:installer_main.cc(475)] Install folder from command line: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2028	58	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installer_main.cc(478)] Uninstall:0	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2086	55	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installer_main.cc(479)] Silent:1	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2141	63	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installer_main.cc(480)] Run Immediately0	success or wait	1	6AD6D6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2204	55	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installer_main.cc(482)] Backend1	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2259	62	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installer_main.cc(483)] Inside package0	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2321	59	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installer_main.cc(484)] Autoupdate:0	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2380	67	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:payload_manager_impl.cc(97)] Reading Payload	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	2447	822	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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 4f 44 64 6b 4e 6a 51 33 5a 57 46 68 5a 47 5a 68 4d 54 51 35 4f 54 67 35 4f 54 59 77 59 7a 67 78 59 6d 4a 6c 4d 6d 51 30 5a 6d 55 32 4e 44 63 78 4f 54 51 35 4f 47 56 6b 4e 7a 4d 79 59 32 59 7a 4d 7a 64 6c 4e 7a 68 6b 5a 47 4a 68 4f 57 56 69 4e 6d 49 33 4d 54 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	[0329/193552.142:INFO:installer_main.cc(610)] Tracking data: ODdkNjQ3ZWFhZGZhMTQ5OTg5OTYwYzgxYmJlMmQ0ZmU2NDcxOTQ5OGVkNzMyY2YzMzdlNzhkZGJhOWViNml3MTp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOi	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3269	88	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:settings_impl.cc(785)] Found 3 paths for standalone install mode.	success or wait	1	6AD6D6C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3357	100	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:resource_l10n_handler.cc(113)] Language not in the available languages list:	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3457	103	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:resource_l10n_handler.cc(119)] Trying language from system preferred list: en-GB	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3560	113	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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 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 6a 6f 6e 65 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	[0329/193552.142:INFO:settings_impl.cc(1327)] Install folder set: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3673	59	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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 33 38 32 29 5d 20 4f 70 65 72 61 74 69 6f 6e 3a 20 31 0a	[0329/193552.142:INFO:settings_impl.cc(1382)] Operation: 1	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3732	64	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installer.cc(196)] Beginning installation	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3796	94	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:permission_grantor_impl.cc(134)] Write privileges for install folder: 1	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3890	88	5b 30 33 32 39 2f 31 39 33 35 35 32 2e 31 34 32 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	[0329/193552.142:INFO:installation_package_impl.cc(70)] Need to wait for actual package	success or wait	1	6AD6D6C3	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	6AC897B8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	3978	74	5b 30 33 32 39 2f 31 39 33 36 31 35 2e 32 36 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	[0329/193615.267:INFO:installation_package_impl.cc(172)] Package is ready	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	4052	1832	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 32 33 36 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 6a 6f 6e 65 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 35 34 32 34 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	[0329/193645.236: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=5424 --install --import-browser-data=0	success or wait	1	6AD6D6C3	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	6AC897B8	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	5884	64	5b 30 33 32 39 2f 31 39 33 37 30 33 2e 37 33 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	[0329/193703.734:INFO:installer.cc(850)] Installation succeeded	success or wait	1	6AD6D6C3	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	5948	95	5b 30 33 32 39 2f 31 39 33 37 30 33 2e 37 33 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	[0329/193703.734:INFO:backend_process_installer_runner_impl.cc(187)] Installer backend exiting	success or wait	1	6AD6D6C3	WriteFile
unknown	unknown	106			invalid handle	2	6AE72B21	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193552126.log	6043	105	5b 30 33 32 39 2f 31 39 33 37 30 33 2e 37 33 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	[0329/193703.734:ERROR:ipc_sender.cc(113)] Cannot write to mailslot: Reached the end of the file. (0x26)	success or wait	2	6AD6D6C3	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	6ADC5259	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	6ADC5259	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\opera_package	0	1024	success or wait	92	6ADF6FFD	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\opera_package	0	3428	success or wait	1	6ADF70FC	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\opera_package	0	16384	success or wait	8647	6ADF70FC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Opera Software	success or wait	1	6AD32680	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	6AEAE859	RegSetValueExW

Analysis Process: OperaGXSetup.exe PID: **2656**, Parent PID: **3716**

General

Target ID:	9
Start time:	19:35:51
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\is-U02B5.tmp\OperaGXSetup.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\is-U02B5.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=0x300,0x304,0x308,0x2d0,0x30c,0x6afc623c,0x6afc6248,0x6afc6254
Imagebase:	0x1000000
File size:	3'581'600 bytes
MD5 hash:	1033B8A679409AAE694776CF2FDD3E8D
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_2403291835520002656.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1002E97	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	6A85E67B	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	6A85E67B	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6A85E67B	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835520002656.dll	success or wait	1	1001979	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291835520002656.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	1002F54	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\crashpad_3716_VNEZNAVIBOJRAWGQ	0	36	success or wait	1	6A875259	ReadFile
\pipe\crashpad_3716_VNEZNAVIBOJRAWGQ	0	36	success or wait	1	6A875259	ReadFile

Analysis Process: Opera_GX_assistant_73.0.3856.382_Setup.exe_sfx.exe PID: **5184**, Parent PID: **5424**

General

Target ID:	10
Start time:	19:36:12
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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_202403291935511\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
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935 511\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_202403291935 511\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_202403291935 511\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_202403291935 511\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_202403291935 511\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_202403291935 511\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 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 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	74	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_202403291935511\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	2	40C086	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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 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_202403291935511\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	4	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_202403291935511\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 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 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.$PELB`"!F@A?t?	success or wait	14	40C086	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\mojo_core.dll	425619	65536	fd 2f 0d 10 fd 44 24 40 68 fd 0e 10 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 49 20 fd 01 5d fd 60 08 fd fd fd fd 55 fd fd 53 57 56 fd 79 74 00 74 71 fd 75 08 fd 56 28 fd fd fd 00 00 00 0f 1f fd 00 00 00 00 00 fd c3 fd 0f 0f fd fd fd 30 0d 10 fd 58 04 fd fd 04 fd fd fd fd fd 75 51 fd 00 00 00 fd 40 04 78 66 fd 40 02 20 30 fd 76 10 0f 1f 40 00 fd fd fd fd 0f 0f fd fd fd 30 0d 10 fd 58 01 fd fd 04 fd fd fd fd fd 75 fd 66 fd 00 30 78 29 fd 52 50 fd 71 74 86 00 00 fd fd 0c 5e 5f 5b 5d fd 04 00 fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 49 20 fd 01 5d fd 60 04 fd fd fd fd 55 fd fd 49 20 fd 01 5d fd 60 18 fd fd fd fd 55 fd fd 53 57 56 fd fd 0c fd cb 55 08 fd fd fd 0b 00 00 fd fd fd 0b 00 00 fd fd 74 27 fd 01 39 fd	/D$@hUI]`USWVyttquV(0Xu@xf@0v@0Xuf0x)RPqt^_[]UI ]`UI]`USWVUt'9	success or wait	1	40C086	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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_202403291935511\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_202403291935511\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_202403291935511\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_202403291935511\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_202403291935511\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_202403291935511\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: **2136**, Parent PID: **5424**

General

Target ID:	11
Start time:	19:36:13
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\assistant_installer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\assistant_installer.exe" --version
Imagebase:	0x2e0000
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	3A5332	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	3A5332	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\assistant_installer_20240329193613.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	32BD0B	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 38 fd fd 49 01 66 56 48 fd 1d fd 41 13 42 30 fd	sdPC8IfVHAB0	success or wait	1	3DA4FA	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 38 fd fd 49 01 66 56 48 fd 1d fd 41 13 42 30 fd	sdPC8IfVHAB0	success or wait	1	3DA4FA	WriteFile
C:\Users\user\AppData\Local\Temp\assistant_installer_20240329193613.log	0	243	5b 30 33 32 39 2f 31 39 33 36 31 33 2e 35 32 34 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 6a 6f 6e 65 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 33 35 35 31 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	[0329/193613.524: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_202403291935511\assistant\assistant_installer.exe" --version	success or wait	1	32C493	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	3DA559	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	3DA559	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	3DA559	ReadFile

Analysis Process: assistant_installer.exe PID: **3128**, Parent PID: **2136**

General	
Target ID:	12
Start time:	19:36:13
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\assistant\assistant_installer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\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,0x494f48,0x494f58,0x494f64
Imagebase:	0x2e0000
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	3A5332	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	3A5332	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	3DA559	ReadFile
\pipe\crashpad_2136_NSHPEITGLQJOWHJX	0	36	success or wait	1	3DA559	ReadFile
\pipe\crashpad_2136_NSHPEITGLQJOWHJX	0	36	success or wait	1	3DA559	ReadFile

Analysis Process: installer.exe PID: **6324**, Parent PID: **3716**

General	
Target ID:	14
Start time:	19:36:45
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=5424 --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_202403291935511" --session-guid=e8c1f83b-82a0-4cf5-8d29-c848e8638bca --server-tracking-blob=ZmUxNWFlNzQyYjk1NzA4ZTljODEyOGM4ZDY1NDg0M2YyNmVhN2MxNjg3MDQ5YmEyMGNjNzFjMzEyNjU5MGZjZTp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9lZGl0aW9uL3N0ZC0xP3V0bV9zb3VyY2U9UFdOZ2FtZXMmdXRtX21lZGl1bT1wYSZ1dG1fY2FtcGFpZ249UFdOX1VTX1BCNF8zNzQyJnV0bV9pZD04NmE3YmY5NzI1Yjk0NDYxYjMzYzMzMGM3ZTA5NDUwMSZ1dG1fY29udGVudD0zNzQyX3NldHVwaW8iLCJzeXN0ZW0iOnsicGxhdGZvcm0iOnsiYXJjaCI6Ing4Nl82NCIsIm9wc3lzIjoiV2luZG93cyIsIm9wc3lzLXZlcnNpb24iOiIxMCIsInBhY2thZ2UiOiJFWEUifX0sInRpbWVzdGFtcCI6IjE3MTE3MzczMjMuMDMxNCIsInVzZXJhZ2VudCI6Ik9wZXJhIEluc3RhbGxlci9Pcy4xLjMyMCIsInV0bSI6eyJjYW1wYWlnbiI6IlBXTl9VU19QQjRfMzc0MiIsImNvbnRlbnQiOiIzNzQyX3NldHVwaW8iLCJpZCI6Ijg2YTdiZjk3MjViOTQ0NjFiMzNjMzMwYzdlMDk0NTAxIiwibWVkaXVtIjoicGEiLCJzb3VyY2UiOiJQV05nYW1lcyJ9LCJ1dWlkIjoiMjAzZWJhZDA2LTcxY2MtNDg4Ny1hOGRmLTdlYTdjNzkwMzhhYSJ9 --silent --desktopshortcut=1 --install-subfolder=107.0.5045.79
Imagebase:	0x7ff709740000
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_2403291836453876324.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF709742DB4	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	7FFDFB6BBC80	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	7FFDFB6BBC80	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	7FFDFB6BBC80	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.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	7FFDFB7F8B18	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	7FFDFB624F2E	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	7FFDFB6593DF	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	7FFDFB624F2E	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	7FFDFB624F2E	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	7FFDFB659AE3	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	7FFDFB624F2E	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFDFB624F2E	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	7FFDFB624F2E	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	7FFDFB659AE3	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	7FFDFB659AE3	CreateFileW
C:\Users\user\AppData\Local\Programs\Opera GX\61fbcc78-252b-40ae-9c42-f61ba1991250.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFDFB657E9E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\launcher.exe.1711737406.old	success or wait	1	7FFDFB658388	DeleteFileW
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list.1711737405.old	success or wait	2	7FFDFB658388	DeleteFileW
C:\Users\user\AppData\Local\Temp\Opera_installer_240329183645387632 4.dll	success or wait	1	7FF709741AD5	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.1711737405.old	success or wait	1	7FFDFB7F14E7	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.1711737405.old	success or wait	1	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	MoveFileExW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	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	7FFDFB7F14E7	MoveFileExW
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	7FFDFB7F14E7	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.1711737406.old	success or wait	1	7FFDFB7F14E7	MoveFileExW
C:\Users\user\AppData\Local\Programs\Opera GX\61fbcc78-252b-40ae-9c42-f61ba1991250.tmp	C:\Users\user\AppData\Local\Programs\Opera GX\installer_prefs.json	success or wait	1	7FFDFB65860C	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Opera_installer_2403291836453876324.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 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	7FF709742C38	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 38 fd fd 49 01 66 56 48 fd 1d fd 41 13 42 30 fd	sdPC8IfVHAB0	success or wait	1	7FFDFB6D941C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	0	105	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 30 39 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	[0329/193645.809:INFO:installer_main.cc(453)] Opera GX installer starting - version 107.0.5045.79 Stable	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	105	1777	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 30 39 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 6a 6f 6e 65 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 35 34 32 34 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	[0329/193645.809:INFO:installer_main.cc(456)] Command line: "C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\installer.exe" --backend --initial-pid=5424 --install --import-browser-data=0 --enable-stats=1 --enable-installer-stats=1 --consent-g	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	1882	127	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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 6a 6f 6e 65 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	[0329/193645.824:INFO:installer_main.cc(475)] Install folder from command line: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2009	58	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:installer_main.cc(478)] Uninstall:0	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2067	55	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:installer_main.cc(479)] Silent:1	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2122	63	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:installer_main.cc(480)] Run Immediately0	success or wait	1	7FFDFB66C10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2185	55	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:installer_main.cc(482)] Backend1	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2240	62	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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 31 0a	[0329/193645.824:INFO:installer_main.cc(483)] Inside package1	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2302	59	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:installer_main.cc(484)] Autoupdate:0	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2361	88	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:settings_impl.cc(785)] Found 3 paths for standalone install mode.	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2449	100	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:resource_l10n_handler.cc(113)] Language not in the available languages list:	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2549	103	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:resource_l10n_handler.cc(119)] Trying language from system preferred list: en-GB	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2652	113	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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 6a 6f 6e 65 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	[0329/193645.824:INFO:settings_impl.cc(1327)] Install folder set: C:\Users\user\AppData\Local\Programs\Opera GX	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2765	59	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:settings_impl.cc(1382)] Operation: 1	success or wait	1	7FFDFB66C10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2824	64	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:installer.cc(196)] Beginning installation	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2888	94	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 32 34 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	[0329/193645.824:INFO:permission_grantor_impl.cc(134)] Write privileges for install folder: 1	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	2982	74	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 38 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	[0329/193645.887:INFO:installation_package_impl.cc(172)] Package is ready	success or wait	1	7FFDFB66C10D	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	7FFDFB55BFE1	WriteFile
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	7FFDFB624F2E	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3056	133	5b 30 33 32 39 2f 31 39 33 36 34 35 2e 39 34 39 3a 49 4e 46 4f 3a 64 65 6c 65 74 65 5f 66 69 6c 65 5f 73 74 65 70 2e 63 63 28 33 32 29 5d 20 44 65 6c 65 74 69 6e 67 20 66 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 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 66 69 6c 65 73 5f 6c 69 73 74 0a	[0329/193645.949:INFO:delete_file_step.cc(32)] Deleting file C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	success or wait	2	7FFDFB66C10D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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.$PEdf"%@`x`	success or wait	6	7FFDFB624F2E	CopyFileW
C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe	0	524288	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 fd 0d 00 fd fd 02 66 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 00 00 2e 1b 00 00 fd 07 00 00 00 00 00 fd fd 12 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 24 00 00 04 00 00 78 2a 23 00 02 00 60 fd 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEdf".@$x*#`	success or wait	5	7FFDFB624F2E	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\Opera GX\server_tracking_data	0	896	5a 6d 55 78 4e 57 46 6c 4e 7a 51 79 59 6a 6b 31 4e 7a 41 34 5a 54 6c 6a 4f 44 45 79 4f 47 4d 34 5a 44 59 31 4e 44 67 30 4d 32 59 79 4e 6d 56 68 4e 32 4d 78 4e 6a 67 33 4d 44 51 35 59 6d 45 79 4d 47 4e 6a 4e 7a 46 6a 4d 7a 45 79 4e 6a 55 35 4d 47 5a 6a 5a 54 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	ZmUxNWFlNzQyYjk1NzA4ZTljODEyOGM4ZDY1NDg0M2YyNmVhN2MxNjg3MDQ5YmEyMGNjNzFjMzEyNjU5MGZjZTp7ImNvdW50cnkiOiJVUyIsImVkaXRpb24iOiJzdGQtMSIsImluc3RhbGxlcl9uYW1lIjoiT3BlcmFHWFNldHVwLmV4ZSIsInByb2R1Y3QiOnsibmFtZSI6Im9wZXJhX2d4In0sInF1ZXJ5IjoiL29wZXJhX2d4L3N0YWJsZS9	success or wait	1	7FFDFB659B47	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\pref_default_overrides	0	2	7b 7d	{}	success or wait	1	7FFDFB624F2E	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3327	71	5b 30 33 32 39 2f 31 39 33 36 34 36 2e 30 37 34 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 73 74 65 70 73 2e 63 63 28 32 35 36 29 5d 20 53 65 74 74 69 6e 67 20 75 70 20 74 68 65 20 72 65 67 69 73 74 72 79 0a	[0329/193646.074:INFO:installer_steps.cc(256)] Setting up the registry	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3398	74	5b 30 33 32 39 2f 31 39 33 36 34 36 2e 31 30 36 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 5f 73 68 6f 72 74 63 75 74 73 5f 73 74 65 70 2e 63 63 28 34 38 29 5d 20 49 6e 73 74 61 6c 6c 69 6e 67 20 73 68 6f 72 74 63 75 74 73 0a	[0329/193646.106:INFO:install_shortcuts_step.cc(48)] Installing shortcuts	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\Desktop\Opera GX Browser .lnk	0	1432	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 0d 08 fd fd 01 fd fd 0d 08 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 76 6b fd 76 fd fd fd 01 fd 21 06 fd 07 fd fd 01 fd 32 fd 0d 08 fd fd 01 14 00 fd 00 74 00 1c 00 43 46 53 46 16 00 31 00 00 00 00 00 43 57 01 5e 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 43 57 01 5e 7d 58 66 fd 2e 00 00 00 fd fd 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 25 04 00 41 00 70 00 70 00 44	LF $:#)#(:DGYr?DUk0&&vkv!2tCFSF1CW^AppDatatY^Hg3(gVAGk@CW^}Xf.%AppD	success or wait	1	7FFDFB624F2E	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Opera GX Browser .lnk	0	1432	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 0d 08 fd fd 01 fd fd 0d 08 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 76 6b fd 76 fd fd fd 01 fd 21 06 fd 07 fd fd 01 fd 32 fd 0d 08 fd fd 01 14 00 fd 00 74 00 1c 00 43 46 53 46 16 00 31 00 00 00 00 00 43 57 01 5e 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 43 57 01 5e 7d 58 66 fd 2e 00 00 00 fd fd 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 25 04 00 41 00 70 00 70 00 44	LF $:#)#(:DGYr?DUk0&&vkv!2tCFSF1CW^AppDatatY^Hg3(gVAGk@CW^}Xf.%AppD	success or wait	1	7FFDFB624F2E	CopyFileW
unknown	unknown	61			invalid handle	1	7FFDFB7A560D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3472	60	5b 30 33 32 39 2f 31 39 33 36 35 31 2e 34 36 35 3a 45 52 52 4f 52 3a 74 61 73 6b 62 61 6e 64 5f 75 74 69 6c 73 5f 69 6d 70 6c 2e 63 63 28 31 31 30 29 5d 20 54 69 6d 65 6f 75 74 0a	[0329/193651.465:ERROR:taskband_utils_impl.cc(110)] Timeout	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3532	152	5b 30 33 32 39 2f 31 39 33 36 35 31 2e 34 36 35 3a 49 4e 46 4f 3a 77 72 69 74 65 5f 69 6e 73 74 61 6c 6c 65 72 5f 70 72 65 66 73 5f 73 74 65 70 2e 63 63 28 35 36 29 5d 20 57 72 69 74 69 6e 67 20 69 6e 73 74 61 6c 6c 65 72 20 70 72 65 66 73 20 74 6f 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 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 69 6e 73 74 61 6c 6c 65 72 5f 70 72 65 66 73 2e 6a 73 6f 6e 0a	[0329/193651.465:INFO:write_installer_prefs_step.cc(56)] Writing installer prefs to C:\Users\user\AppData\Local\Programs\Opera GX\installer_prefs.json	success or wait	1	7FFDFB66C10D	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_202403291935511\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	7FFDFB7F13BC	CopyFileW
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3684	76	5b 30 33 32 39 2f 31 39 33 36 35 31 2e 39 31 38 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 5f 65 78 74 72 61 5f 61 70 70 73 5f 73 74 65 70 2e 63 63 28 35 31 29 5d 20 49 6e 73 74 61 6c 6c 69 6e 67 20 65 78 74 72 61 20 61 70 70 73 0a	[0329/193651.918:INFO:install_extra_apps_step.cc(51)] Installing extra apps	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\installation_status.json	0	12856	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 37 34 30 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":"1711737405","copy_only":false,"files":["107.0.5045.79.manifest","CUESDK.x64_2017.dll","MEIPreload\\manifest.json","MEIPreload\\preloaded_data	success or wait	1	7FFDFB659B47	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3760	71	5b 30 33 32 39 2f 31 39 33 36 35 32 2e 31 30 36 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 5f 73 74 65 70 73 2e 63 63 28 33 39 37 29 5d 20 43 72 65 61 74 69 6e 67 20 73 63 68 65 64 75 6c 65 64 20 74 61 73 6b 0a	[0329/193652.106:INFO:installer_steps.cc(397)] Creating scheduled task	success or wait	1	7FFDFB66C10D	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	7FFDFB659B47	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3831	76	5b 30 33 32 39 2f 31 39 33 36 35 32 2e 33 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 2e 63 63 28 36 31 39 29 5d 20 46 69 6e 61 6c 69 7a 69 6e 67 20 73 75 63 63 65 73 73 66 75 6c 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 0a	[0329/193652.371:INFO:installer.cc(619)] Finalizing successful installation	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	3907	155	5b 30 33 32 39 2f 31 39 33 36 35 32 2e 33 37 31 3a 49 4e 46 4f 3a 69 6e 73 74 61 6c 6c 65 72 2e 63 63 28 31 31 38 29 5d 20 4c 61 75 6e 63 68 69 6e 67 20 6f 70 65 72 61 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 6a 6f 6e 65 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 6c 61 75 6e 63 68 65 72 2e 65 78 65 22 20 2d 2d 73 74 61 72 74 2d 6d 61 78 69 6d 69 7a 65 64 0a	[0329/193652.371:INFO:installer.cc(118)] Launching opera with command line "C:\Users\user\AppData\Local\Programs\Opera GX\launcher.exe" --start-maximized	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Programs\Opera GX\61fbcc78-252b-40ae-9c42-f61ba1991250.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	7FFDFB657587	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	4062	64	5b 30 33 32 39 2f 31 39 33 37 30 30 2e 33 37 31 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	[0329/193700.371:INFO:installer.cc(850)] Installation succeeded	success or wait	1	7FFDFB66C10D	WriteFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer\opera_installer_20240329193645809.log	4126	95	5b 30 33 32 39 2f 31 39 33 37 30 30 2e 33 37 31 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	[0329/193700.371:INFO:backend_process_installer_runner_impl.cc(187)] Installer backend exiting	success or wait	1	7FFDFB66C10D	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	7FFDFB6D94B1	ReadFile
C:\Users\user\AppData\Roaming\Opera Software\Opera GX Stable\Crash Reports\settings.dat	0	40	success or wait	1	7FFDFB6D94B1	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	0	4096	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	0	4096	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\files_list	0	4096	end of file	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list	0	4096	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\root_files_list	0	4096	end of file	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\files_list	0	4096	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\files_list	0	4096	end of file	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\pref_default_overrides	0	4096	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\pref_default_overrides	0	4096	end of file	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\installer_prefs_include.json	0	4096	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Temp\.opera\Opera GX Installer Temp\opera_package_202403291935511\installer_prefs_include.json	0	4096	end of file	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	0	1343488	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	0	4096	success or wait	1	7FFDFB79F979	ReadFile
C:\Users\user\AppData\Local\Programs\Opera GX\107.0.5045.79\resources\custom_partner_content.json	0	4096	end of file	1	7FFDFB79F979	ReadFile

Analysis Process: installer.exe PID: **6936**, Parent PID: **6324**

General

Target ID:	15
Start time:	19:36:45
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=0x2c0,0x2c4,0x2c8,0x29c,0x2cc,0x7ffdfb93d180,0x7ffdfb93d18c,0x7ffdfb93d198
Imagebase:	0x7ff709740000
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: **2580**, Parent PID: **6324**

General

Target ID:	18
Start time:	19:36:48
Start date:	29/03/2024
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff72b770000

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: rrcsBizXUHISSeck.exe PID: **1704**, Parent PID: **6324**

General

Target ID:	19
Start time:	19:36:50
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
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: rrcsBizXUHISSeck.exe PID: **5668**, Parent PID: **6324**

General

Target ID:	20
Start time:	19:36:50
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
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: rrcsBizXUHISSeck.exe PID: **2896**, Parent PID: **6324**

General

Target ID:	21
Start time:	19:36:51
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717

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

Analysis Process: rrcsBizXUHISSeck.exe PID: **4020**, Parent PID: **6324**

General	
Target ID:	22
Start time:	19:36:51
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: rrcsBizXUHISSeck.exe PID: **1004**, Parent PID: **6324**

General	
Target ID:	23
Start time:	19:36:51
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: rrcsBizXUHISSeck.exe PID: **1456**, Parent PID: **6324**

General	
Target ID:	24
Start time:	19:36:51
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: rrcsBizXUHISSeck.exe PID: **4996**, Parent PID: **6324**

General	
Target ID:	25
Start time:	19:36:51
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: rrcsBizXUHISSeck.exe PID: **5300**, Parent PID: **6324**

General	
Target ID:	26
Start time:	19:36:51
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: rrcsBizXUHISSeck.exe PID: **5676**, Parent PID: **6324**

General	
Target ID:	27
Start time:	19:36:52
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: rrcsBizXUHISSeck.exe PID: **3808**, Parent PID: **6324**

General	
Target ID:	28

Start time:	19:36:52
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: launcher.exe PID: **4900**, Parent PID: **6324**

General	
Target ID:	29
Start time:	19:36:52
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:	0x7ff6ed480000
File size:	2'304'416 bytes
MD5 hash:	D737A64C835D918DBE53B2C7724488FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: rrcsBizXUHISSeck.exe PID: **3004**, Parent PID: **6324**

General	
Target ID:	30
Start time:	19:36:52
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: launcher.exe PID: **2932**, Parent PID: **1044**

General	
Target ID:	31
Start time:	19:36:53
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:	0x7ff6ed480000
File size:	2'304'416 bytes
MD5 hash:	D737A64C835D918DBE53B2C7724488FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: opera_gx_splash.exe PID: **4820**, Parent PID: **4900**

General	
Target ID:	32
Start time:	19:36:54
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=0e78e69c624cbcf87c7f299659eb65c0
Imagebase:	0x7ff7e8be0000
File size:	2'231'200 bytes
MD5 hash:	706FE814240C22A6CB09FBF48CB86020
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: opera.exe PID: **5252**, Parent PID: **4900**

General	
Target ID:	33
Start time:	19:36:55
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=0e78e69c624cbcf87c7f299659eb65c0 --splash-handle=1040
Imagebase:	0x7ff602c00000
File size:	1'508'256 bytes
MD5 hash:	F452A15BC7E4392149F6BB2675EAAA59
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: rrcsBizXUHISSeck.exe PID: **2648**, Parent PID: **6324**

General	
Target ID:	34
Start time:	19:36:56
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false

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

Analysis Process: rrcsBizXUHISSeck.exe PID: **2852**, Parent PID: **6324**

General

Target ID:	35
Start time:	19:36:56
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: opera_crashreporter.exe PID: **6412**, Parent PID: **5252**

General

Target ID:	36
Start time:	19:36:56
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,0x280,0x290,0x7ffdf2ce9628,0x7ffdf2ce9638,0x7ffdf2ce9648
Imagebase:	0x7ff677700000
File size:	2'019'744 bytes
MD5 hash:	26DF88B2E68E23B60C0EEAB3E29496BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: rrcsBizXUHISSeck.exe PID: **6012**, Parent PID: **6324**

General

Target ID:	37
Start time:	19:36:57
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Has exited:	false

Analysis Process: opera.exe PID: **6668**, Parent PID: **2580**

General	
Target ID:	38
Start time:	19:36:57
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=0e78e69c624cbcf87c7f299659eb65c0 --splash-handle=1040 --lowered-browser
Imagebase:	0x7ff602c00000
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:	false

Analysis Process: installer.exe PID: **6692**, Parent PID: **2932**

General	
Target ID:	39
Start time:	19:36:57
Start date:	29/03/2024
Path:	C:\Users\user\AppData\Local\Temp\.opera\BDDCE5348F09\installer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\.opera\BDDCE5348F09\installer.exe" --version
Imagebase:	0x7ff631f00000
File size:	6'949'792 bytes
MD5 hash:	21AD4599ABD2E158DB5128F32D3CC4EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: rrcsBizXUHISSeck.exe PID: **3584**, Parent PID: **6324**

General	
Target ID:	40
Start time:	19:36:57
Start date:	29/03/2024
Path:	C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\jxonYJeoGHBcEBBtArQrvhEwKtVoDVDAGPqvUohUoVEGcPnsXlHYZHnvjNxJfSEodCXJXYDjNppAXMAN\rrcsBizXUHISSeck.exe"
Imagebase:	0x5a0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Disassembly

No disassembly