ID: 1440170
Sample Name: file.exe
Cookbook: default.jbs
Time: 12:46:06
Date: 12/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

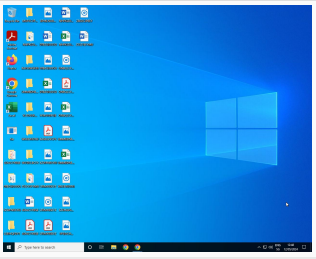
Windows Analysis Report

file.exe

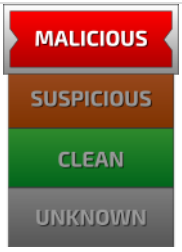
Overview

General Information

Sample name:	file.exe
Analysis ID:	1440170
MD5:	43b0461d2e1c…
SHA1:	96c50c5b2d65…
SHA256:	d4536f1b7e5fb…
Tags:	exe
Infos:	



Detection



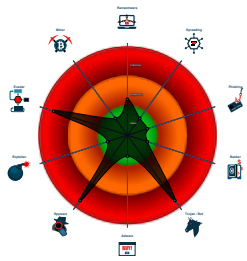
PrivateLoader, Vidar

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Yara detected AntiVM3
- Yara detected PrivateLoader
- Yara detected Vidar
- Yara detected Vidar stealer
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Contains functionality to inject code…
- Found many strings related to Crypt…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 2520 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 43B0461D2E1C77A8530D66D3E1AE0175)
  - conhost.exe (PID: 4180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - RegAsm.exe (PID: 2832 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
    - cmd.exe (PID: 7700 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\BGDAAKJJDAAK" & exit MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 7712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - timeout.exe (PID: 7756 cmdline: timeout /t 10 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
PrivateLoader	According to sekoia, PrivateLoader is a modular malware whose main capability is to download and execute one or several payloads. The loader implements anti-analysis techniques, fingerprints the compromised host and reports statistics to its C2 server.	No Attribution	**http://** https://any.run/cybersecurity-blog/crackedcantil-breakdown/https://any.run/cybersecurity-blog/privateloader-analyzing-the-encryption-and-decryption-of-a-modern-loader/https://bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadeyhttps://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.privateloader

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	**http**://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

Threatname: Vidar


```
{
  "C2 url": [
    "https://steamcommunity.com/profiles/76561199681720597"
  ],
  "Botnet": "681a223bec180ebfdc48547d3d5bd784",
  "Version": "9.6"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
sslproxydump.pcap	JoeSecurity_Vidar_2	Yara detected Vidar	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\BGDAAKJJDAAK\vcruntime140.dll	JoeSecurity_PrivateLoader	Yara detected PrivateLoader	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\vcruntime140[1].dll	JoeSecurity_PrivateLoader	Yara detected PrivateLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.2170451919.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2170451919.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x221f0:$s1: JohnDoe • 0x32f80:$s1: JohnDoe • 0x221e8:$s2: HAL9TH
00000000.00000002.1610588292.0000000000705000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RegAsm.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.RegAsm.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x20ff0:$s1: JohnDoe • 0x20fe8:$s2: HAL9TH
2.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.RegAsm.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x221f0:$s1: JohnDoe • 0x32f80:$s1: JohnDoe • 0x221e8:$s2: HAL9TH
0.2.file.exe.630000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Spreading

Yara detected PrivateLoader

Networking

Yara detected PrivateLoader

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Searches for specific processes (likely to inject)

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected PrivateLoader

Yara detected Vidar

Yara detected Vidar stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Opens network shares

Tries to harvest and steal Bitcoin Wallet information

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Crypto Currency Wallets

Remote Access Functionality

Yara detected PrivateLoader

Yara detected Vidar

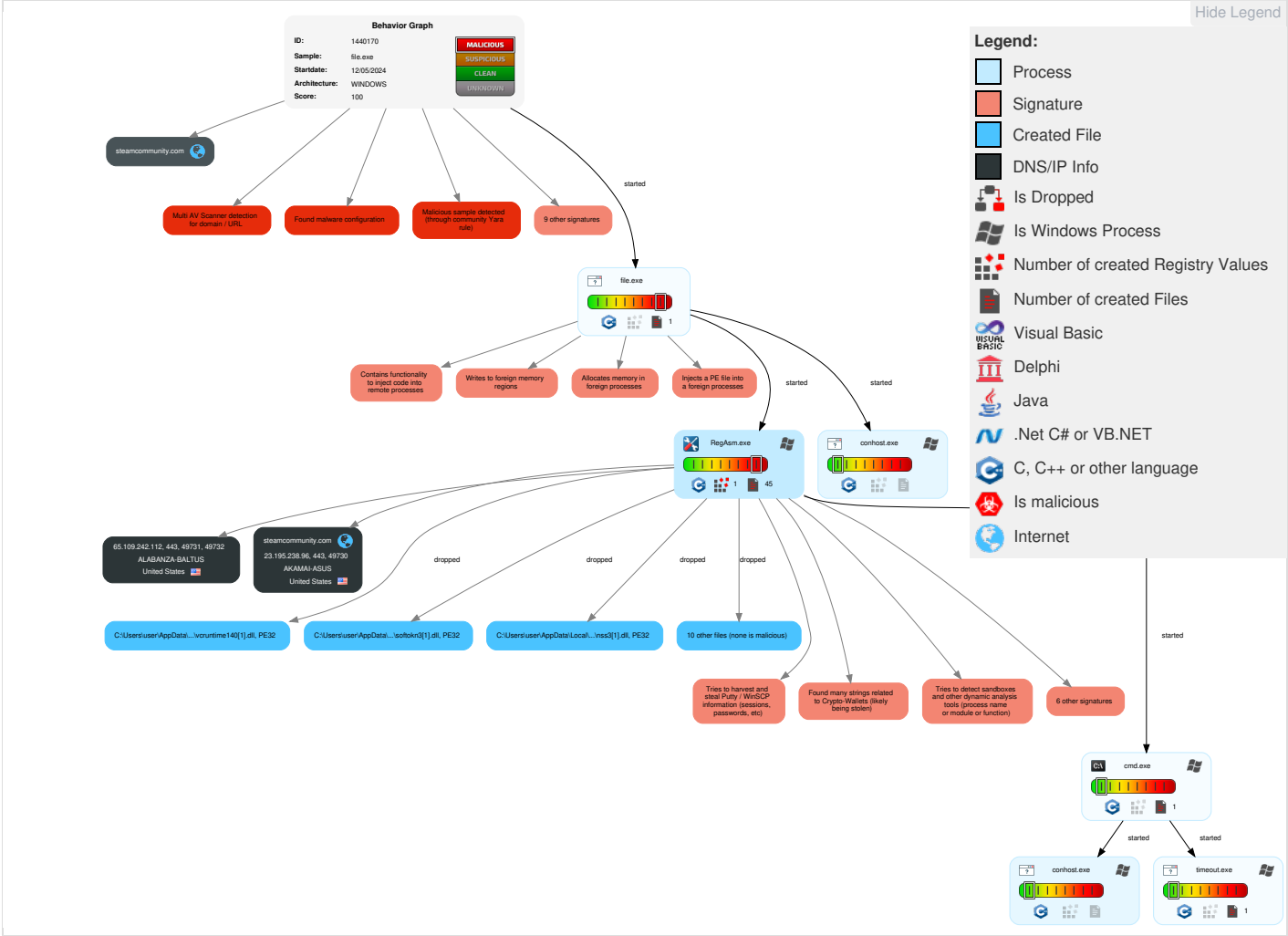
Yara detected Vidar stealer

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	Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	2 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	Boot or Logon Initialization Scripts	5 1 1 Process Injection	2 Obfuscated Files or Information	1 Credentials in Registry	1 Account Discovery	Remote Desktop Protocol	4 Data from Local System	2 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	4 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Masquerading	NTDS	5 6 System Information Discovery	Distributed Component Object Model	Input Capture	1 1 4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Virtualization/Sandbox Evasion	LSA Secrets	1 Network Share Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	5 1 1 Process Injection	Cached Domain Credentials	1 4 1 Security Software Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 2 Process Discovery	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	HTML Smuggling	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement

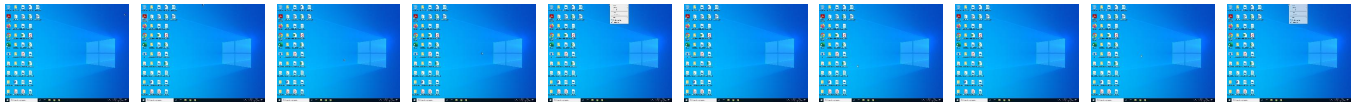
Behavior Graph

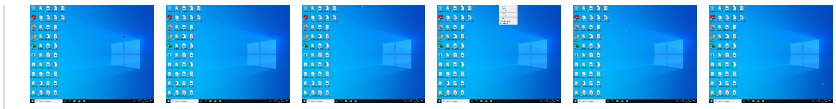


Screenshots

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
file.exe	100%	Avira	HEUR/AGEN.1318539	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\BGDAAKJJDAAK\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\BGDAAKJJDAAK\freebl3.dll	0%	Virustotal		Browse
C:\ProgramData\BGDAAKJJDAAK\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\BGDAAKJJDAAK\mozglue.dll	0%	Virustotal		Browse
C:\ProgramData\BGDAAKJJDAAK\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\BGDAAKJJDAAK\msvcp140.dll	0%	Virustotal		Browse
C:\ProgramData\BGDAAKJJDAAK\nss3.dll	0%	ReversingLabs		
C:\ProgramData\BGDAAKJJDAAK\nss3.dll	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\ProgramData\BGDAAKJJDAAK\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\BGDAAKJJDAAK\softokn3.dll	0%	Virustotal		Browse
C:\ProgramData\BGDAAKJJDAAK\vcruntime140.dll	0%	ReversingLabs		
C:\ProgramData\BGDAAKJJDAAK\vcruntime140.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\freebl3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\freebl3[1].dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\mozglue[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\mozglue[1].dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\msvcp140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\msvcp140[1].dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\nss3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\nss3[1].dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\softokn3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\softokn3[1].dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\vcruntime140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\vcruntime140[1].dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://imp.mt48.net/static?id=7RHzfOIXjFEYsBdvlpkX4QqmfZfYfQfafZbXfpbWfpbX7ReNxR3UIG8zInwYIFIVs9eYi	0%	URL Reputation	safe	
http://https://mozilla.org0/	0%	URL Reputation	safe	
http://https://mozilla.org0/	0%	URL Reputation	safe	
http://https://bridge.lga1.ap01.net/ctp?version=16.0.0&key=1696332238301000001.1&ci=1696332238417.12791&cta	0%	URL Reputation	safe	
http://https://65.109.242.112/freebl3.dllo	0%	Avira URL Cloud	safe	
http://store.st	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/nss3.dllMsi	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/softokn3.dllM	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/msvcp140.dll	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/freebl3.dll	0%	Avira URL Cloud	safe	
http://https://65.109.242.112	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/sqlx.dll	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/softokn3.dll	0%	Avira URL Cloud	safe	
http://https://65.109.242.112HJJ	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/mozglue.dll	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/mozglue.dlle	0%	Avira URL Cloud	safe	
http://https://65.109.242.112	12%	Virustotal		Browse
http://https://65.109.242.112/	12%	Virustotal		Browse
http://https://65.109.242.112/p	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/nss3.dll	0%	Avira URL Cloud	safe	
http://https://65.109.242.112JDG	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/#	0%	Avira URL Cloud	safe	
http://https://65.109.242.112/sqlx.dll	11%	Virustotal		Browse
http://https://65.109.242.112/#	12%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
steamcommunity.com	23.195.238.96	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://65.109.242.112/msvcp140.dll	false	• Avira URL Cloud: safe	unknown
http://https://65.109.242.112/freebl3.dll	false	• Avira URL Cloud: safe	unknown
http://https://65.109.242.112/vcruntime140.dll	false	• Avira URL Cloud: safe	unknown
http://https://65.109.242.112/sqlx.dll	false	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://65.109.242.112/	false	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://65.109.242.112/softokn3.dll	false	• Avira URL Cloud: safe	unknown
http://https://65.109.242.112/mozglue.dll	false	• Avira URL Cloud: safe	unknown
http://https://65.109.242.112/nss3.dll	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/profiles/76561199681720597	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	EBAFBG.2.dr	false		high
http://https://duckduckgo.com/ac/?q=	EBAFBG.2.dr	false		high
http://https://steamcommunity.com/?subsection=broadcasts	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://65.109.242.112/nss3.dllMsi	RegAsm.exe, 00000002.00000002.2171023727.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bridge.lga1.admarketplace.net/ctp?version=16.0.0&key=1696332238301000001.2&ci=1696332238417.	RegAsm.exe, 00000002.00000002.2171023727.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp, GHCGDA.2.dr	false		high
http://https://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/libraries~b28b7af6	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/modalContent.js?v=L35TrLJDfqtD&l=engl	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/main.js?v=ZQOnBoEs	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://www.valvesoftware.com/legal.htm	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/promo/summer2017/stickers.css?v=HA2Yr5oy3FFG&	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://65.109.242.112/softokn3.dllM	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.png	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://steamcommunity.com/profiles/76561199681720597GL	RegAsm.exe, 00000002.00000002.2171023727.0000000000F50000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://imp.mt48.net/static?id=7RHzfOIXjFEYsBdvIpkX4QqmfZfYfQfafZbXfpbWfpbX7ReNxR3UIG8zInwYIFIVs9eYi	GHCGDA.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIlcMzCffX6&	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://steamcommunity.com/profiles/76561199681720597/badges	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/profile.js?v=Iy1ies1ROjUT&l=english	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://t.me/talmatin	file.exe, 00000000.00000002.1610588292.000000000705000.00000004.00000001.01000000.00000003.sdmp, RegAsm.exe, RegAsm.exe, 00000002.00000002.2170451919.000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://www.amazon.com/?tag=admarketus-20&ref=pd_sl_7548d4575af019e4c148ccf1a78112802e66a0816a72fc94	RegAsm.exe, 00000002.00000002.2171023727.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp, GHCGDA.2.dr	false		high
http://www.mozilla.com/en-US/blocklist/	RegAsm.exe, RegAsm.exe, 00000002.00000002.2178967195.000000006F90D000.00000002.00000001.01000000.00000008.sdmp, mozglue[1].dll.2.dr, mozglue.dll.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/skin_1/header.css?v=NFoCa4OkAxRb&l=english	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://mozilla.org0/	freebl3.dll.2.dr, nss3[1].dll.2.dr, softokn3[1].dll.2.dr, softokn3.dll.2.dr, mozglue[1].dll.2.dr, mozglue.dll.2.dr, nss3.dll.2.dr, freebl3[1].dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown

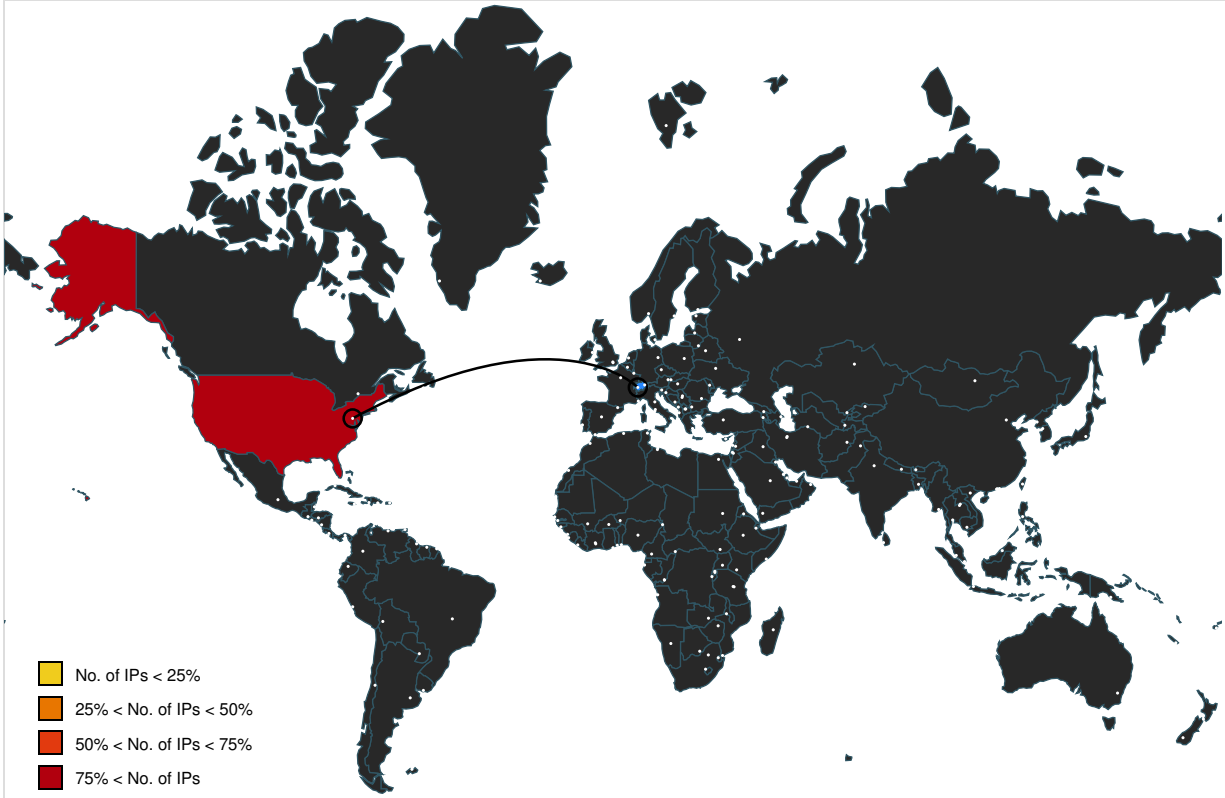
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%2	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp	false		high
http://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://store.st	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/profiles/76561199681720597/inventory/	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://store.steampowered.com/points/shop/	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	EBAFBG.2.dr	false		high
http://https://bridge.lga1.ap01.net/ctp?version=16.0.0&key=16963322383010000001.1&ci=1696332238417.12791&cta	RegAsm.exe, 00000002.00000002.2171023727.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp, GHCGDA.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=qzBY	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://65.109.242.112/freebl3.dllo	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	RegAsm.exe, 00000002.00000002.2170451919.000000000060E000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.0000000000574000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://www.ecosia.org/newtab/	EBAFBG.2.dr	false		high
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	AEHIEC.2.dr	false		high
http://https://avatars.akamai.steamstatic.com/fef49e7fa7e1997310d705b2a6158ff8dc1cdfeb_full.jpg	76561199681720597[1].htm.2.dr	false		high
http://https://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_global.js?v=REEGJU1hwkYI&am	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199681720597	76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=english	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://65.109.242.112	76561199681720597[1].htm.2.dr	false	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_logo.png	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://store.steampowered.com/about/	76561199681720597[1].htm.2.dr	false		high
http://https://steamcommunity.com/my/wishlist/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	AEHIEC.2.dr	false		high
http://https://steamcommunity.com/profiles/76561199681720597eL	RegAsm.exe, 00000002.00000002.2171023727.0000000000F50000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://help.steampowered.com/en/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://steamcommunity.com/market/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://store.steampowered.com/news/	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	EBAFBG.2.dr	false		high
http://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://65.109.242.112HJJ	RegAsm.exe, 00000002.00000002.2170451919.0000000000530000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://community.akamai.steamstatic.com/public/javascript/promo/stickers.js?v=upl9NJ5D2xkP&l=en	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://steamcommunity.com/discussions/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://65.109.242.112/mozglue.dlle	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.steampowered.com/stats/	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://store.steampowered.com/steam_refunds/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/webui/clientcom.js?v=yXrh2LzpDwct&l=e	RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://65.109.242.112/p	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	EBAFBG.2.dr	false		high
http://https://steamcommunity.com/workshop/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://store.steampowered.com/legal/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&l=e	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000002.00000002.2175331068.000000001B68D000.00000002.00001000.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2172015655.00000000156E7000.00000004.00000020.00020000.00000000.sdmp, sqlx[1].dll.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v=pSv	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=engl	76561199681720597[1].htm.2.dr	false		high
http://https://contile-images.services.mozilla.com/0TegrVVRalreHILhR2WvtD_CFzj13HCDcLqqpvXSOuY.10862.jpg	RegAsm.exe, 00000002.00000002.2171023727.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp, GHCGDA.2.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	EBAFBG.2.dr	false		high
http://https://65.109.242.112JDG	RegAsm.exe, 00000002.00000002.2170451919.0000000000574000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://store.steampowered.com/	76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016ost.exe	RegAsm.exe, 00000002.00000002.2170451919.0000000000574000.00000040.00000400.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://65.109.242.112/#	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp	false	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/images/skin_1/arrowDn9x5.gif	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://ac.ecosia.org/autocomplete?q=	EBAFBG.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://https://contile-images.services.mozilla.com/obgoOYObjIFea_bXuT6L4LbBJ8j425AD87S1HMD3BWg.9991.jpg	RegAsm.exe, 00000002.00000002.2171023727.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp, GHCGDA.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/buttons.css?v=PUJIfhtcQn7W&l=english	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high
http://store.steampowered.com/account/cookiepreferences/	RegAsm.exe, 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2170451919.000000000043D000.00000040.00000400.00020000.00000000.sdmp, 76561199681720597[1].htm.2.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.195.238.96	steamcommunity.com	United States		16625	AKAMAI-ASUS	false
65.109.242.112	unknown	United States		11022	ALABANZA-BALTUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1440170
Start date and time:	2024-05-12 12:46:06 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	file.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/25@1/2
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SIHClient.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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.

Simulations

Behavior and APIs

Time	Type	Description
12:47:01	API Interceptor	1x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\BGDAAKJJDAAK\AEHIEC

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622
SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F3176B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>..

C:\ProgramData\BGDAAKJJDAAK\AEHIEC-shm

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.017262956703125623
Encrypted:	false
SSDEEP:	3:G8lQs2TSlElQs2TtPRp//:G0QjSaQjrpX
MD5:	B7C14EC6110FA820CA6B65F5AEC85911
SHA1:	608EEB7488042453C9CA40F7E1398FC1A270F3F4
SHA-256:	FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
SHA-512:	D8D75760F29B1E27AC9430BC4F4FFCEC39F1590BE5AEF2BFB5A535850302E067C288EF59CF3B2C5751009A22A6957733F9F80FA18F2B0D33D90C068A3F08F3B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..-.....8...5.....-.....8...5.....

C:\ProgramData\BGDAAKJJDAAK\BGDAAK

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1

Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A
SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4457 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\BGDAAKJJDAAK\EBAFBG

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\ProgramData\BGDAAKJJDAAK\ECFHCG

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 11, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.5793180405395284
Encrypted:	false
SSDEEP:	96:/xealJiyIsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7Yltnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621(3
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\ProgramData\BGDAAKJJDAAK\FCFIJE

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cook ie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153

Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE361789045928
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....}..}.....

C:\ProgramData\BGDAAKJJDAAK\FCFIJE-shm

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.017262956703125623
Encrypted:	false
SSDEEP:	3:G8lQs2TSlElQs2TtPRp//:G0QjSaQjrpX
MD5:	B7C14EC6110FA820CA6B65F5AEC85911
SHA1:	608EEB7488042453C9CA40F7E1398FC1A270F3F4
SHA-256:	FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
SHA-512:	D8D75760F29B1E27AC9430BC4F4FFCEC39F1590BE5AEF2BFB5A535850302E067C288EF59CF3B2C5751009A22A6957733F9F80FA18F2B0D33D90C068A3F08F3B
Malicious:	false
Preview:	..-.....8...5.....-.....8...5.....

C:\ProgramData\BGDAAKJJDAAK\FIDAFC

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\ProgramData\BGDAAKJJDAAK\GHCGDA

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with very long lines (1809), with CRLF line terminators
Category:	dropped
Size (bytes):	9571
Entropy (8bit):	5.536643647658967
Encrypted:	false
SSDEEP:	192:qnaRt+YbBp6ihj4qyaaX86KKkfGNBw8DJSl:yegqumcwQ0
MD5:	5D8E5D85E880FB2D153275FCBE9DA6E5
SHA1:	72332A8A92B77A8B1E3AA00893D73FC2704B0D13
SHA-256:	50490DC0D0A953FA7D5E06105FE9676CDB9B49C399688068541B19DD911B90F9
SHA-512:	57441B4CCBA58F557E08AAA0918D1F9AC36D0AF6F6EB3D3C561DA7953ED156E89857FFB829305F65D220AE1075BC825F131D732B589B5844C82CA90B53AAF4E

Malicious:	false
Preview:	// Mozilla User Preferences....// DO NOT EDIT THIS FILE...//..// If you make changes to this file while the application is running,..// the changes will be overwritten when the application exits...//..// To change a preference value, you can either:..// - modify it via the UI (e.g. via about:config in the browser); or..// - set it within a user.js file in your profile.....user_pref("app.normandy.first_run", false);..user_pref("app.normandy.migrationsApplied", 12);..user_pref("app.normandy.user_id", "57f16a19-e119-4073-bf01-28f88011f783");..user_pref("app.update.auto.migrated", true);..user_pref("app.update.background.rolledout", true);..user_pref("app.update.lastUpdateTime.browser-cleanup-thumbnails", 0);..user_pref("app.update.lastUpdateTime.recipe-client-addon-run", 1696333830);..user_pref("app.update.lastUpdateTime.region-update-timer", 0);..user_pref("app.update.lastUpdateTime.rs-experiment-loader-timer", 1696333856);..user_pref("app.update.lastUpdateTime.xpi-signature-verification

C:\ProgramData\BGDAAKJJDAAK\IDBKKK

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F79838
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\BGDAAKJJDAAK\IIEBAF

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\ProgramData\BGDAAKJJDAAK\freebl3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	685392
Entropy (8bit):	6.872871740790978
Encrypted:	false
SSDEEP:	12288:4gPbPpxMofhPNN0+RXBrp3M5pzRN4l2SQ+PEu9tUs/abAQb51FW/IzkOfWPO9UN7:4gPbPp9NNP0BgInfW2WMC4M+hW
MD5:	550686C0EE48C386DFCB40199BD076AC
SHA1:	EE5134DA4D3EFCB466081FB6197BE5E12A5B22AB
SHA-256:	EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
SHA-512:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....4.....p.....@A.... .....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F.. .0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..."..... .....@..B..... .....

C:\ProgramData\BGDAAKJJDAAK\mozglue.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.833616094889818
Encrypted:	false
SSDEEP:	12288:BlSyAom/gcRKMdRm4wFkRHuyG4RRGJVDjMk/x21R8gY/r:BKgcRKMdRm4wFkVVDGJVv//x21R8br
MD5:	C8FD9BE83BC728CC04BEFFAFC2907FE9
SHA1:	95AB9F701E0024CEDFBD312BCFE4E726744C4F2E
SHA-256:	BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
SHA-512:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B40
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..L....4.c....."!.....^.....j.....@A.... .....`...W.....P/...0...A...S.....h.....Z.....text...a..... ..`.rdata.....@..@.data...D..... .....@....00cfg.....@..@.tls.....@....rsrc..... .....@..@.reloc...A...0...B.....@..B..... .....

C:\ProgramData\BGDAAKJJDAAK\msvcp140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	450024
Entropy (8bit):	6.673992339875127
Encrypted:	false
SSDEEP:	12288:McPa9C9VbL+3Omy5CvyOvzeOKdqhUgiW6QR7t5s03Ooc8dHkC2esGAWf:McPa90Vbky5CvyUeOKn03Ooc8dHkC2eN
MD5:	5FF1FCA37C466D6723EC67BE93B51442
SHA1:	34CC4E158092083B13D67D6D2BC9E57B798A303B
SHA-256:	5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
SHA-512:	4802EF62630C521D83A1D333969593FB00C9B38F82B4D07F70FBD21F495FEA9B3F67676064573D2C71C42BC6F701992989742213501B16087BB6110E337C7546
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._...._..._.)n...._.....,_...^."._..^..._..\..._..[..._..Z..._..._..._.....,_..]..._.Rich.._.....PE..L.....0]....."!.....(.....`.....@.....,....@A.....g.....r.....A.....=..`x..8.....w ..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc..... .....Z.....@..@.reloc...=.....>...^.....@..B..... .....

C:\ProgramData\BGDAAKJJDAAK\nss3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2046288
Entropy (8bit):	6.787733948558952
Encrypted:	false
SSDEEP:	49152:fECf12gikHlnKGxJRIB+y5nvxnaOSJ3HFNWYrVvE4CQsgzMmQfTU1NrWmy4KoAzh:J7Tf8J1Q+SS5/nr
MD5:	1CC453CDF74F31E4D913FF9C10ACDDE2
SHA1:	6E85EAE544D6E965F15FA5C39700FA7202F3AAFE
SHA-256:	AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5
SHA-512:	DD9FF4E06B00DC831439BAB11C10E9B2AE864EA6E780D3835EA7468818F35439F352EF137DA111EFCDF2BB6465F6CA486719451BF6CF32C6A4420A56B1D64571
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..L....4.c....."!.....`.....p.....l- ...@A.... .....&.....@....P..x.....P/...`..\.....|..\....&..@.....text..... ..`.rdata..l.....@..@.data...DR.. .....@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\...`.....@..B..... ....

C:\ProgramData\BGDAAKJJDAAK\softokn3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	257872
Entropy (8bit):	6.727482641240852
Encrypted:	false
SSDEEP:	6144:/yF/zX2zfRkU62THVh/T2AhZxv6A31obD6Hq/8jis+FvtVRpsAAs0o8OqTYz+xnU:/yRzX2zfRkX2T1h/SA5PF9m8jJqKYz+y
MD5:	4E52D739C324DB8225BD9AB2695F262F
SHA1:	71C3DA43DC5A0D2A1941E874A6D015A071783889
SHA-256:	74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
SHA-512:	2D4168A69082A9192B9248F7331BD806C260478FF817567DF54F997D7C3C7D640776131355401E4BDB9744E246C36D658CB24B18DE67D8F23F10066E5FE445F6
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..L....4.c....."!.....P.....Sg ....@A.....Dv..S....w.....P/.....5..8q.....{.....text...&..... ..`.rdata.....@..@.da ta.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... ....

C:\ProgramData\BGDAAKJJDAAK\vcruntime140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80880
Entropy (8bit):	6.920480786566406
Encrypted:	false
SSDEEP:	1536:lw2886xv555et/MCsjw0BuRK3jteo3ecbA2W86b+Ld:lw28V55At/zqw+lq9ecbA2W8H
MD5:	A37EE36B536409056A86F50E67777DD7
SHA1:	1CAFA159292AA736FC595FC04E16325B27CD6750
SHA-256:	8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825
SHA-512:	3A7C260646315CF8C01F44B2EC60974017496BD0D80DD055C7E43B707CADBA2D63AAB5E0EFD435670AA77886ED86368390D42C4017FC433C3C4B9D1C47D0F3 6
Malicious:	false
Yara Hits:	• Rule: JoeSecurity_PrivateLoader, Description: Yara detected PrivateLoader, Source: C:\ProgramData\BGDAAKJJDAAK\vcruntime140.dll, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L...|.0].....!.....0.....m....@A.....A... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199681720597[1].htm

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (2969), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	34771
Entropy (8bit):	5.3843653404896905
Encrypted:	false
SSDEEP:	768:Edpqm+0Ih3YAA9CWGIWfcDAoPzzgiJmDzJtxvrfJkPVoEAdmPzzgiJmDzJtxvJ28:Ed8m+0Ih3YAA9CWGIWFoPzzgiJmDzJt/
MD5:	B8719A1861962262D390617FEC83C72E
SHA1:	1CAFE529AF3EE421C5A478F3404C4748D6D95C4D
SHA-256:	A762A4EB54C1E217B0466FCB48B569E5928F0DB2C4E09B07207908EF49F3DA7C

SHA-512:	D746C3AAC9045C6EE0D63C4FA24D0B2690992472F0A98A1BF9405919E5A3F6C3EF19AB1DF75472BA6CCCD88325ADCFF8C75E3DA0C4CB33920FE630850629C0B3
Malicious:	false
Preview:	<!DOCTYPE html>..<html class=" responsive" lang="en">..<head>...<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.....<meta name="viewport" content="width=device-width,initial-scale=1">....<meta name="theme-color" content="#171a21">....<title>Steam Community :: p5.r https://65.109.242.112|</title>...<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">.....<link href="https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/buttons.css?v=PUJIfhtcQn7W&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english" rel="stylesheet" type="text/css" >.<link hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2459136
Entropy (8bit):	6.052474106868353
Encrypted:	false
SSDEEP:	49152:WHoJ9zGioiMjW2RrL9B8SSpiCH7cuez9A:WHoJBGqabRnj8JY/9
MD5:	90E744829865D57082A7F452EDC90DE5
SHA1:	833B178775F39675FA4E55EAB1032353514E1052
SHA-256:	036A57102385D7F0D7B2DEACF932C1C372AE30D924365B7A88F8A26657DD7550
SHA-512:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E57032
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.Z.Y.Z.Y.Z.Y...Z.n.Y...\..Y...]...Y...X.Y.Y.Z.X..Y.O.\.E.Y.O.].U.Y.O.Z.L.Y.l3].[.Y.l3Y.[.Y.l3..[.Y.l3[.[.Y.RichZ.Y.....PE..L...i.`e.....!...%.. .....{D..... .....%.....@.....#..6....$.(....$.....$....`.#.8.....x.#.@.....$.....text...G. ....`.rdata..."....$.... .....@..@.data...4|... $..b....#.....@....idata.....$.....^$.....@..@.00cfg.....$.....p$.....@..@.rsrc.....$.....r$.....@..@.reloc..5.....$.....$.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\freebl3[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	685392
Entropy (8bit):	6.872871740790978
Encrypted:	false
SSDEEP:	12288:4gPbPpxMofhPNN0+RXBrp3M5pzRN4l2SQ+PEu9tUs/abAQb51FW/IzkOfWPO9UN7:4gPbPp9NNP0BgInfW2WMC4M+hW
MD5:	550686C0EE48C386DFCB40199BD076AC
SHA1:	EE5134DA4D3EFCB466081FB6197BE5E12A5B22AB
SHA-256:	EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
SHA-512:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....4.....p.....@A.....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F..0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..."....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\mozglue[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.833616094889818
Encrypted:	false
SSDEEP:	12288:BlSyAom/gcRKMdRm4wFkRHuyG4RRGJVDjMk/x21R8gY/r:BKgcRKMdRm4wFkVVDGJVv//x21R8br
MD5:	C8FD9BE83BC728CC04BEFFAFC2907FE9
SHA1:	95AB9F701E0024CEDFBD312BCFE4E726744C4F2E

SHA-256:	BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
SHA-512:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B40
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..L....4.c....."!.....^.....j.....@A.....`...W.....P/...0...A...S.....h.....Z.....text...a..... ..`.rdata.....@..@.data...D.....@....00cfg.....@..@.tls.....@....rsrc..... .....@..@.reloc...A...0...B.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\msvcp140[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	450024
Entropy (8bit):	6.673992339875127
Encrypted:	false
SSDEEP:	12288:McPa9C9VbL+3Omy5CvyOvzeOKdqhUgiW6QR7t5s03Ooc8dHkC2esGAWf:McPa90Vbky5CvyUeOKn03Ooc8dHkC2eN
MD5:	5FF1FCA37C466D6723EC67BE93B51442
SHA1:	34CC4E158092083B13D67D6D2BC9E57B798A303B
SHA-256:	5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
SHA-512:	4802EF62630C521D83A1D333969593FB00C9B38F82B4D07F70FBD21F495FEA9B3F67676064573D2C71C42BC6F701992989742213501B16087BB6110E337C7546
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._...._..._)n...._....._...^."._.^..._.\..._..[..._..Z..._..._....._..]..._.Rich.._.....PE..L.....0]....."!.....(.....`.....@.....,....@A.....g.....r.....A.....=..`x..8.....w..@.....p.....c..@.....text...&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc.....Z.....@..@.reloc...=.....>...^.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\nss3[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2046288
Entropy (8bit):	6.787733948558952
Encrypted:	false
SSDEEP:	49152:fECf12gikHlnKGxJRIB+y5nvxnaOSJ3HFNWYrVvE4CQsgzMmQfTU1NrWmy4KoAzh:J7Tf8J1Q+SS5/nr
MD5:	1CC453CDF74F31E4D913FF9C10ACDDE2
SHA1:	6E85EAE544D6E965F15FA5C39700FA7202F3AAFE
SHA-256:	AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5
SHA-512:	DD9FF4E06B00DC831439BAB11C10E9B2AE864EA6E780D3835EA7468818F35439F352EF137DA111EFCDF2BB6465F6CA486719451BF6CF32C6A4420A56B1D64571
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..L....4.c....."!.....`.....p.....l- ...@A.....&.....@....P..x.....P/...`..\.....|...\....&..@.....text..... ..`.rdata..l.....@..@.data...DR..@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\....`.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\softokn3[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	257872
Entropy (8bit):	6.727482641240852
Encrypted:	false
SSDEEP:	6144:/yF/zX2zfRkU62THVh/T2AhZxv6A31obD6Hq/8jis+FvtVRpsAAs0o8OqTYz+xnU:/yRzX2zfRkX2T1h/SA5PF9m8jJqKYz+y
MD5:	4E52D739C324DB8225BD9AB2695F262F

SHA1:	71C3DA43DC5A0D2A1941E874A6D015A071783889
SHA-256:	74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
SHA-512:	2D4168A69082A9192B9248F7331BD806C260478FF817567DF54F997D7C3C7D640776131355401E4BDB9744E246C36D658CB24B18DE67D8F23F10066E5FE445F6
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..L....4.c....."!.....P.....Sg ....@A.....Dv..S....w.....P/.....5..8q.....{.....text...&..... ..`.rdata.....@..@.da ta.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\vcruntime140[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80880
Entropy (8bit):	6.920480786566406
Encrypted:	false
SSDEEP:	1536:lw2886xv555et/MCsjw0BuRK3jteo3ecbA2W86b+Ld:lw28V55At/zqw+lq9ecbA2W8H
MD5:	A37EE36B536409056A86F50E67777DD7
SHA1:	1CAFA159292AA736FC595FC04E16325B27CD6750
SHA-256:	8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825
SHA-512:	3A7C260646315CF8C01F44B2EC60974017496BD0D80DD055C7E43B707CADBA2D63AAB5E0EFD435670AA77886ED86368390D42C4017FC433C3C4B9D1C47D0F36
Malicious:	false
Yara Hits:	• Rule: JoeSecurity_PrivateLoader, Description: Yara detected PrivateLoader, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\vcruntime140[1].dll, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L...|.0]....."!.....0.....m....@A.....A... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.328959132341708
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	1'153'024 bytes
MD5:	43b0461d2e1c77a8530d66d3e1ae0175
SHA1:	96c50c5b2d652a572e18147e213e8bea38118f94
SHA256:	d4536f1b7e5fbfdfe66be6a404147230dcff7728bc559b493d7bdd8e1adaea08
SHA512:	4ec4add62526c8f2e2119d6043de7494040c86bdb5cceb973fdfd8131e287e0ef52560626fabc66220de1539531e0592683f5e16cb03f384b08f16b4729ad6bd
SSDEEP:	24576:t4HFil+p/dJqGunDHUX/wMsWZfbDR9ceqHKUZAs:t4lzJqGunDH6l59gKUZAs
TLSH:	F3359E3139C09176EEE310B787ECBA29866DD0B0075911DF57D85AEED720AC27F32686
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t}.50..f0..f0..f.n.g<..f.n.g...f.n.g%..f.n.g3..f0..fm..f...g"..f...g$..f...g...f...g1..f...g1..fRich0..f.....PE..L..

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x4011e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x66408D4D [Sun May 12 09:35:09 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	0d00e7b5922fb5549ed71add897d60ba

Entrypoint Preview

Instruction
jmp 00007FAC310FD3ABh
jmp 00007FAC311239D7h
jmp 00007FAC310FC8B3h
jmp 00007FAC311058D1h
jmp 00007FAC310EF8AAh
jmp 00007FAC310D9D91h
jmp 00007FAC311626A2h
jmp 00007FAC310EFE57h
jmp 00007FAC31124755h
jmp 00007FAC311672C4h
jmp 00007FAC310D5119h
jmp 00007FAC310FDF8Ah
jmp 00007FAC310D3DADh
jmp 00007FAC3110E3FEh
jmp 00007FAC310E824Ah
jmp 00007FAC310CBF95h
jmp 00007FAC31111C16h
jmp 00007FAC310D7551h
jmp 00007FAC310D0556h
jmp 00007FAC3115363Ah
jmp 00007FAC310CB7CCh
jmp 00007FAC310CAAD7h
jmp 00007FAC3111EEEEh
jmp 00007FAC3113B876h
jmp 00007FAC310EC40Eh
jmp 00007FAC3115F3EAh
jmp 00007FAC3112CED2h
jmp 00007FAC310F805Ch
jmp 00007FAC3110648Ch
jmp 00007FAC310CE65Fh
jmp 00007FAC31137680h
jmp 00007FAC31160134h
jmp 00007FAC310E6219h
jmp 00007FAC310FE8E3h
jmp 00007FAC31111BD2h
jmp 00007FAC3115BB26h
jmp 00007FAC3114A613h

Instruction
jmp 00007FAC310CB44Ah
jmp 00007FAC3114778Eh
jmp 00007FAC310E8733h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1171e8	0x28	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x119000	0x4a98	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xcc070	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xcbf88	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x117000	0x1e8	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

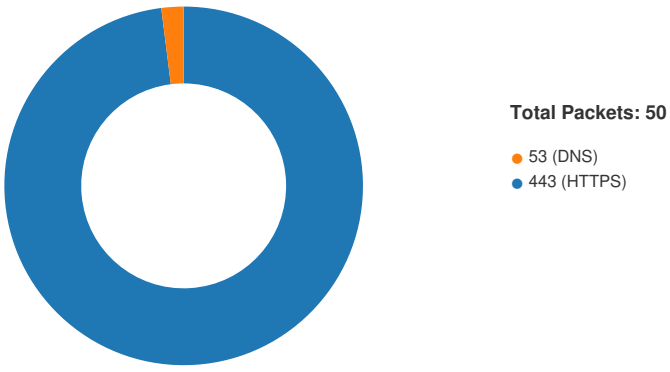
Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xbc163	0xbc200	b725058dd53b7d7dedb65938fce17658	False	0.3306945598006645	data	5.789897639087584	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.bss	0xbe000	0xd7b	0xe00	74d38ec06459bd131b05e4b9c14491d4	False	0.45982142857142855	data	5.465199311557537	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xbf000	0x156d7	0x15800	cefbc46009fd83df37132eaff20d485b	False	0.2858489280523256	DIY-Thermocam raw data (Lepton 3.x), scale 28160-24832, spot sensor temperature 0.000000, unit celsius, color scheme 0, calibration: offset 10141204801825835211973625643008.000000, slope 148078355747941908480.000000	3.698556344652708	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd5000	0x41efc	0x40400	27b49b746c2806fd7f8c16b5cfd5ab85	False	0.8076133876459144	data	7.203012112153988	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x117000	0xc85	0xe00	2f5de5d5db33e473a3669f61cedae18a	False	0.330078125	data	4.394738779870993	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.00cfg	0x118000	0x10e	0x200	dd7371b36f5a16d74de96b27a869ea73	False	0.03515625	data	0.11055713125913882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x119000	0x57c9	0x5800	06eb18e3f1b1c805484fb0d559442570	False	0.6424893465909091	data	6.073709849462629	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	WaitForSingleObject, ExitProcess, CreateThread, VirtualAlloc, GetModuleHandleA, GetProcAddress, FreeConsole, FormatMessageA, WideCharToMultiByte, MultiByteToWideChar, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, LocalFree, GetLocaleInfoEx, EncodePointer, DecodePointer, LCMapStringEx, CompareStringEx, GetCPInfo, IsProcessorFeaturePresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, WriteConsoleW, RaiseException, RtlUnwind, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameW, GetModuleHandleExW, GetCommandLineA, GetCommandLineW, GetCurrentThread, HeapFree, HeapAlloc, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetFileType, CloseHandle, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, SetConsoleCtrlHandler, GetTimeZoneInformation, OutputDebugStringW, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, SetStdHandle, GetProcessHeap, CreateFileW, HeapSize, SetEndOfFile

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:46:52.401218891 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:52.401262045 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:52.401319981 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:52.408319950 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:52.408334970 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:52.743246078 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:52.743346930 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:52.791008949 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:52.791027069 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:52.791277885 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:52.791338921 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:52.794734955 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:52.836123943 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.238809109 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.238827944 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.238868952 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.238902092 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.238919973 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.238945007 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.238969088 CEST	49730	443	192.168.2.4	23.195.238.96

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:46:53.397507906 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.397555113 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.397593975 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.397608995 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.397620916 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.397648096 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.425898075 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.425934076 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.425955057 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.425967932 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.426009893 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.518044949 CEST	49730	443	192.168.2.4	23.195.238.96
May 12, 2024 12:46:53.518065929 CEST	443	49730	23.195.238.96	192.168.2.4
May 12, 2024 12:46:53.532818079 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:53.532849073 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:53.532910109 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:53.533174992 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:53.533186913 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:54.552495003 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:54.552571058 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:54.557092905 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:54.557105064 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:54.557327986 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:54.557385921 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:54.558120012 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:54.600116014 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.201886892 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.201947927 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.202071905 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.204788923 CEST	49731	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.204799891 CEST	443	49731	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.207150936 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.207179070 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.207261086 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.207463026 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.207478046 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.868297100 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.868391037 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.868787050 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.868794918 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:55.871567011 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:55.871572018 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:56.951169014 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:56.951231956 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:56.951417923 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:56.951419115 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:56.951646090 CEST	49732	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:56.951658010 CEST	443	49732	65.109.242.112	192.168.2.4
May 12, 2024 12:46:56.953077078 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:56.953114033 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:56.953176975 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:56.953427076 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:56.953437090 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:57.605804920 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:57.605874062 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:57.606493950 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:57.606507063 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:57.608217955 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:57.608222008 CEST	443	49733	65.109.242.112	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:46:58.679732084 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:58.679753065 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:58.679826975 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:58.679910898 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:58.680149078 CEST	49733	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:58.680166006 CEST	443	49733	65.109.242.112	192.168.2.4
May 12, 2024 12:46:58.681684017 CEST	49734	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:58.681715012 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:46:58.681797981 CEST	49734	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:58.682025909 CEST	49734	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:58.682040930 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:46:59.340619087 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:46:59.340712070 CEST	49734	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:59.341113091 CEST	49734	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:59.341121912 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:46:59.342811108 CEST	49734	443	192.168.2.4	65.109.242.112
May 12, 2024 12:46:59.342816114 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:47:00.434700012 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:47:00.434722900 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:47:00.434777021 CEST	443	49734	65.109.242.112	192.168.2.4
May 12, 2024 12:47:00.434803009 CEST	49734	443	192.168.2.4	65.109.242.112

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2024 12:46:52.229378939 CEST	49963	53	192.168.2.4	1.1.1.1
May 12, 2024 12:46:52.392379999 CEST	53	49963	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 12, 2024 12:46:52.229378939 CEST	192.168.2.4	1.1.1.1	0xea63	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false

DNS Answers

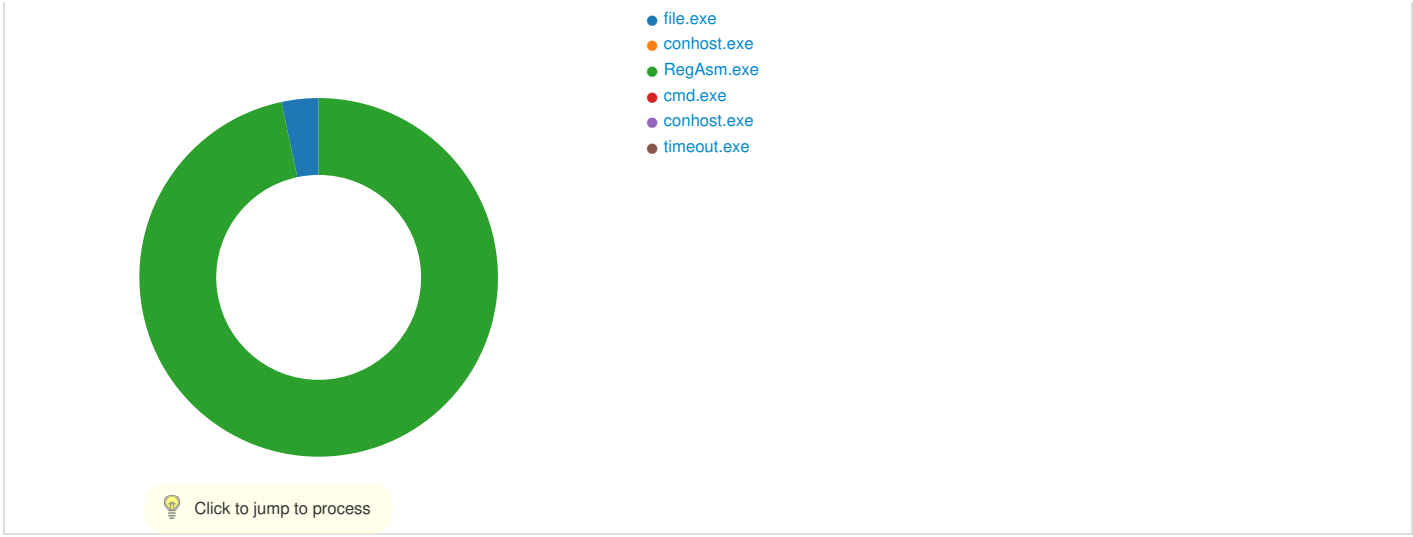
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 12, 2024 12:46:52.392379999 CEST	1.1.1.1	192.168.2.4	0xea63	No error (0)	steamcommunity.com		23.195.238.96	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com
- 65.109.242.112

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 2520, Parent PID: 2580

General

Target ID:	0
Start time:	12:46:50
Start date:	12/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x630000
File size:	1'153'024 bytes
MD5 hash:	43B0461D2E1C77A8530D66D3E1AE0175
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.1610588292.0000000000705000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: 4180, Parent PID: 2520

General

Target ID:	1
Start time:	12:46:50
Start date:	12/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: **2832**, Parent PID: **2520**

General

Target ID:	2
Start time:	12:46:51
Start date:	12/05/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
Imagebase:	0x890000
File size:	65'440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000002.00000002.2170451919.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000002.00000002.2170451919.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.2171023727.0000000000F80000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	416C5C	CreateDirectoryA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
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	405072	HttpSendRequestA
C:\ProgramData\BGDAAKJJDAAK\ECFHCG	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	406901	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	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	40D22D	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	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	40C3D2	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\EBAFBG	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	40CF94	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\IDBKKK	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	40D22D	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\BGDAAK	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	40C3D2	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\FIDAFC	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	40CF94	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EC1	CreateFileA
C:\ProgramData\BGDAAKJJDAAK\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EC1	CreateFileA
C:\ProgramData\BGDAAKJJDAAK\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EC1	CreateFileA
C:\ProgramData\BGDAAKJJDAAK\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EC1	CreateFileA
C:\ProgramData\BGDAAKJJDAAK\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EC1	CreateFileA
C:\ProgramData\BGDAAKJJDAAK\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EC1	CreateFileA
C:\ProgramData\BGDAAKJJDAAK\FCFIJE	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	40889A	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\FCFIJE-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B454EE7	CreateFileW
C:\ProgramData\BGDAAKJJDAAK\FCFIJE-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B454EE7	CreateFileW
C:\ProgramData\BGDAAKJJDAAK\AEHIEC	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	409276	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\AEHIEC-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B454EE7	CreateFileW
C:\ProgramData\BGDAAKJJDAAK\AEHIEC-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B454EE7	CreateFileW
C:\ProgramData\BGDAAKJJDAAK\GHCGDA	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	40B71F	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\ECFHCG	success or wait	1	406E18	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	success or wait	1	40D323	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	success or wait	1	40C670	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\EBAFBG	success or wait	1	40D114	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\IDBKKK	success or wait	1	40D323	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\BGDAAK	success or wait	1	40C670	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\FIDAFC	success or wait	1	40D114	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\FCFIJE-shm	success or wait	1	1B455612	DeleteFileW
C:\ProgramData\BGDAAKJJDAAK\FCFIJE-wal	success or wait	1	1B455612	DeleteFileW
C:\ProgramData\BGDAAKJJDAAK\FCFIJE	success or wait	1	408CFD	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\AEHIEC-shm	success or wait	2	1B455612	DeleteFileW
C:\ProgramData\BGDAAKJJDAAK\AEHIEC	success or wait	1	4094D3	DeleteFileA
C:\ProgramData\BGDAAKJJDAAK\GHCGDA	success or wait	1	40B7F4	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199681720597[1].htm	0	1999	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 20 72 65 73 70 6f 6e 73 69 76 65 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0d 0a 09 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 68 65 6d 65 2d 63 6f 6c 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 23 31 37 31 61 32 31 22 3e 0d 0a 09 09 3c	<!DOCTYPE html><html class=" responsive" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1"><meta name="theme-color" content="#171a21"><	success or wait	18	405116	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	0	1024	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 08 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 1e fd 37 fd 5a fd 59 fd 5a fd 59 fd 5a fd 59 fd 11 fd 5a fd 6e fd 59 fd 11 fd 5c fd f3 59 fd 11 fd 5d fd 7f fd 59 fd 11 fd 58 fd 59 fd 59 fd 5a fd 58 fd 33 59 fd 4f fd 5c fd 45 fd 59 fd 4f fd 5d fd 55 fd 59 fd 4f fd 5a fd 4c fd 59 fd 6c 33 5d fd 5b fd 59 fd 6c 33 59 fd 5b fd 59 fd 6c 33 fd fd 5b fd 59 fd 6c 33 5b fd 5b fd 59 fd 52 69 63 68 5a fd 59 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7ZYZYZYZnY\Y] Y XYYZXYO\EYO]UYOZLY l3][Yl3Y[Yl3[Yl3[[YRichZY	success or wait	2331	404366	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\ECFHCG	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0b 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	406901	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 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 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	2	40D22D	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 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 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	40C3D2	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\EBAFBG	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	40CF94	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\IDBKKK	0	126976	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40D22D	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\BGDAAK	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 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 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40C3D2	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\FIDAFC	0	114688	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 38 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 8$.O}4	success or wait	1	40CF94	CopyFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\freebl3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	629	404F0C	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\freebl3.dll	0	1024	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 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 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 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	670	404EE8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\mozglue[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	557	404F0C	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\mozglue.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 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 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	594	404EE8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\msvcp140[1].dll	0	1024	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 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 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^_ _[_Z_____]_Rich_	success or wait	413	404F0C	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\msvcp140.dll	0	1024	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 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 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	440	404EE8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\nss3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1917	404F0C	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\nss3.dll	0	1024	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 06 00 fd 34 12 63 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 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 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1999	404EE8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\softokn3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	237	404F0C	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\softokn3.dll	0	1024	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 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 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 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	252	404EE8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZJCZETOO\vcruntime140[1].dll	0	1024	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 fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd 0e fd fd fd fd fd 0f fd fd fd fd fd 0a fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"	success or wait	75	404F0C	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\vcruntime140.dll	0	1024	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 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 fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"	success or wait	79	404EE8	WriteFile
C:\ProgramData\BGDAAKJJDAAK\FCFIJE	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	1	40889A	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJDAAK\AEHIEC	0	524288	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAs qpqp{ooh nnemn,m9lklPjjhhgdcc6b baa>	success or wait	10	409276	CopyFileA
C:\ProgramData\BGDAAKJJDAAK\GHCGDA	0	9571	2f 2f 20 4d 6f 7a 69 6c 6c 61 20 55 73 65 72 20 50 72 65 66 65 72 65 6e 63 65 73 0d 0a 0d 0a 2f 2f 20 44 4f 20 4e 4f 54 20 45 44 49 54 20 54 48 49 53 20 46 49 4c 45 2e 0d 0a 2f 2f 0d 0a 2f 2f 20 49 66 20 79 6f 75 20 6d 61 6b 65 20 63 68 61 6e 67 65 73 20 74 6f 20 74 68 69 73 20 66 69 6c 65 20 77 68 69 6c 65 20 74 68 65 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 69 73 20 72 75 6e 6e 69 6e 67 2c 0d 0a 2f 2f 20 74 68 65 20 63 68 61 6e 67 65 73 20 77 69 6c 6c 20 62 65 20 6f 76 65 72 77 72 69 74 74 65 6e 20 77 68 65 6e 20 74 68 65 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 65 78 69 74 73 2e 0d 0a 2f 2f 0d 0a 2f 2f 20 54 6f 20 63 68 61 6e 67 65 20 61 20 70 72 65 66 65 72 65 6e 63 65 20 76 61 6c 75 65 2c 20 79 6f 75 20 63 61 6e 20 65 69 74 68 65 72 3a 0d 0a 2f 2f 20 2d	// Mozilla User Preferences// DO NOT EDIT THIS FILE.//// If you make changes to this file while the application is running,// the changes will be overwritten when the application exits.//// To change a preference value, you can either:// -	success or wait	1	40B71F	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	66646	success or wait	1	406259	ReadFile
C:\ProgramData\BGDAAKJJDAAK\ECFHCG	0	100	success or wait	6	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	0	100	success or wait	6	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	0	100	success or wait	6	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\IIEBAF	0	100	success or wait	6	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\EBAFBG	0	100	success or wait	9	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\EBAFBG	0	100	success or wait	18	1B44FE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	406259	ReadFile
C:\ProgramData\BGDAAKJJDAAK\IDBKKK	0	100	success or wait	12	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\BGDAAK	0	100	success or wait	6	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\FIDAFC	0	100	success or wait	20	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\FCFIJE	0	100	success or wait	4	1B44FE09	ReadFile
C:\ProgramData\BGDAAKJJDAAK\AEHIEC	0	100	success or wait	5	1B44FE09	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	66646	success or wait	1	406259	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	406259	ReadFile
C:\ProgramData\BGDAAKJJDAAK\GHCGDA	0	9571	success or wait	1	406259	ReadFile
C:\ProgramData\BGDAAKJJDAAK\GHCGDA	0	9571	success or wait	1	406259	ReadFile

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **7700**, Parent PID: **2832**

General

Target ID:	6
Start time:	12:47:46
Start date:	12/05/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\BGDAAKJJDAAK" & exit
Imagebase:	0x240000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7712**, Parent PID: **7700**

General

Target ID:	7
Start time:	12:47:47
Start date:	12/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: **7756**, Parent PID: **7700**

General

Target ID:	8
Start time:	12:47:47
Start date:	12/05/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 10
Imagebase:	0xf50000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly