ID: 1442218
Sample Name: file.exe
Cookbook: default.jbs
Time: 20:35:06
Date: 15/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

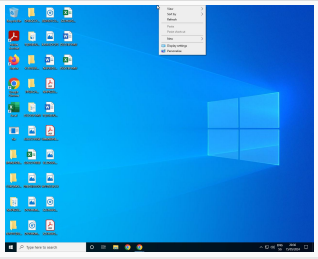
Windows Analysis Report

file.exe

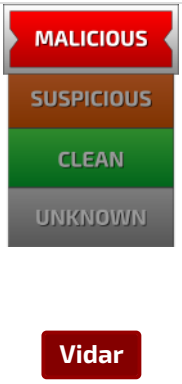
Overview

General Information

Sample name:	file.exe
Analysis ID:	1442218
MD5:	b580ff2d00129…
SHA1:	5013dc6e38bd…
SHA256:	80994b791b54…
Tags:	exe
Infos:	



Detection



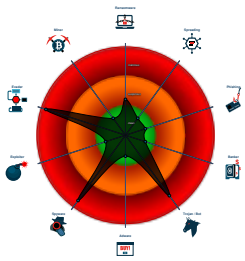
Vidar

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Powershell download…
- 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: 6856 cmdline: "C:\Users\user\Desktop\file.exe" MD5: B580FF2D001291BF58BDD23A058EF21B)
  - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - RegAsm.exe (PID: 3272 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
  - RegAsm.exe (PID: 5984 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
    - cmd.exe (PID: 2860 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\GHIJJEGDBFII" & exit MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 3412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - timeout.exe (PID: 2116 cmdline: timeout /t 10 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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/76561199686524322"
  ],
  "Botnet": "9ed287469c3721fd5caf346580b2cf0d",
  "Version": "9.7"
}
```


Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.2039421679.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000003.00000002.2039421679.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x221f0:$s1: JohnDoe • 0x31f80:$s1: JohnDoe • 0x221e8:$s2: HAL9TH
00000000.00000002.1589701895.000000000070A000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000003.00000002.2039421679.0000000000572000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.70aac0.1.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.file.exe.70aac0.1.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x201f0:$s1: JohnDoe • 0x201e8:$s2: HAL9TH
3.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
3.2.RegAsm.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x221f0:$s1: JohnDoe • 0x31f80:$s1: JohnDoe • 0x221e8:$s2: HAL9TH
0.2.file.exe.70aac0.1.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 5 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

Antivirus detection for URL or domain

Found malware configuration

Machine Learning detection for sample

Networking

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

Yara detected Powershell download and execute

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 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

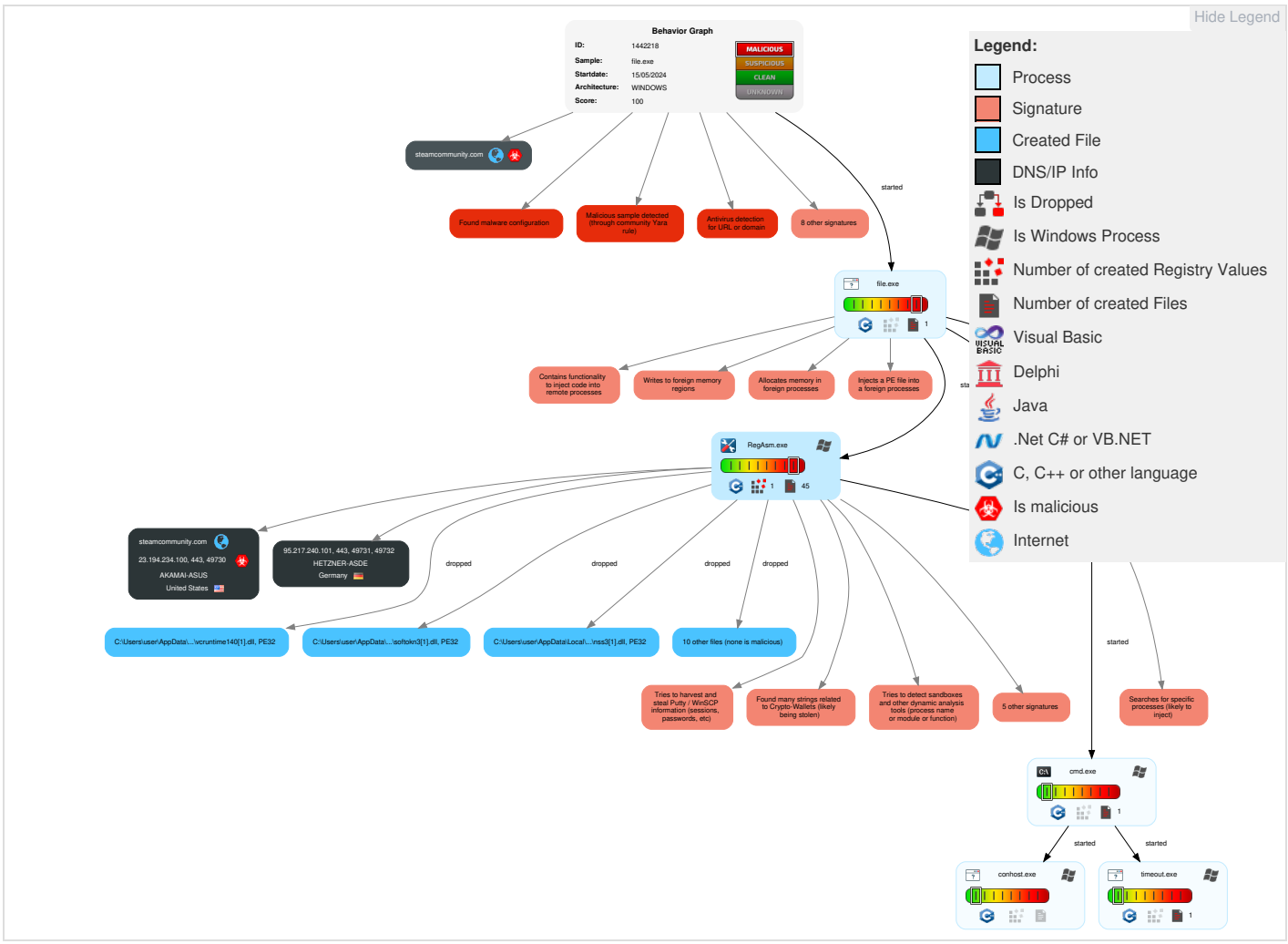
Yara detected Vidar

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	2 Command and Scripting Interpreter	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 5 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
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.1317471	
file.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bridge.lga1.admarketplace.net/ctp?version=16.0.0&key=1696332238301000001.2&ci=1696332238417.	0%	URL Reputation	safe	
http://https://store.steampowered.com/subscriber_agreement/	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=engli	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpE	0%	URL Reputation	safe	
http://www.valvesoftware.com/legal.htm	0%	URL Reputation	safe	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	0%	URL Reputation	safe	
http://https://imp.mt48.net/static?id=7RHzfOIXjFEYsBdvIpkX4QqmfZfYfQfafZbXfpbWfpbX7ReNxR3UIG8zInwYIFIVs9eYi	0%	URL Reputation	safe	
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	0%	URL Reputation	safe	
http://https://www.amazon.com/?tag=admarketus-20&ref=pd_sl_7548d4575af019e4c148ccf1a78112802e66a0816a72fc94	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh&	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/modalContent.js?v=Wd0kCESeJquW&l=	0%	URL Reputation	safe	
http://www.mozilla.com/en-US/blocklist/	0%	URL Reputation	safe	
http://https://mozilla.org0/	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw&	0%	URL Reputation	safe	
http://store.steampowered.com/privacy_agreement/	0%	URL Reputation	safe	
http://https://store.steampowered.com/points/shop/	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://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	0%	URL Reputation	safe	
http://https://store.steampowered.com/privacy_agreement/	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/libraries~b28b	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/header_logo.png	0%	URL Reputation	safe	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	0%	URL Reputation	safe	
http://https://store.steampowered.com/about/	0%	URL Reputation	safe	
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC&	0%	URL Reputation	safe	
http://https://help.steampowered.com/en/	0%	URL Reputation	safe	
http://https://store.steampowered.com/news/	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://store.steampowered.com/subscriber_agreement/	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/manifest.js?v=	0%	URL Reputation	safe	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	0%	URL Reputation	safe	
http://https://steamcommunity.co	100%	Sophos S4	illegal phishing domain	
http://https://store.steampowered.com/stats/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0&	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/webui/clientcom.js?v=dERfFkkJ-bKK&	0%	Avira URL Cloud	safe	
http://https://store.steampowered.com/steam_refunds/	0%	URL Reputation	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/images/skin_1/arrowDn9x5.gif	0%	URL Reputation	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/nss3.dll	100%	Avira URL Cloud	malware	
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/shared_global.js?v=wJD9maDpDcV	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v	0%	URL Reputation	safe	
http://https://steamcommunity.com/?subsection=broadcasts	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/nss3.dll2	100%	Avira URL Cloud	malware	
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/tooltip.j	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/promo/stickers.js?v=GfA42_x2_aub&	0%	Avira URL Cloud	safe	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.p	0%	URL Reputation	safe	
http://https://store.steampowered.com/legal/	0%	URL Reputation	safe	
http://www.sqlite.org/copyright.html.	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/css/buttons.css?v=tuNiaSwXwcYT&l=engl	0%	URL Reputation	safe	
http://https://95.217.240.101/freebl3.dll	100%	Avira URL Cloud	malware	
http://https://community.cloudflare.steamstatic.com/public/shared/css/motiva_sans.css?v=GfSjbGKcNYaQ&l=	0%	URL Reputation	safe	
http://https://contile-images.services.mozilla.com/0TegrVVRalreHILhR2WvtD_CFzj13HCDcLqqpvXSOuY.10862.jpg	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/header.css?v=vh4BMeDcNiCU&l=engli	0%	URL Reputation	safe	
http://https://store.steampowered.com/	0%	URL Reputation	safe	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016ost.exe	0%	URL Reputation	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://community.cloudflare.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	0%	URL Reputation	safe	
http://https://contile-images.services.mozilla.com/obgoOYObjIFea_bXuT6L4LbBJ8j425AD87S1HMD3BWg.9991.jpg	0%	URL Reputation	safe	
http://https://95.217.240.101KJE	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/login	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199686524322	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/css/promo/summer2017/stickers.css?v=bZKSp7oNwVPK	0%	Avira URL Cloud	safe	
http://https://95.217.240.101FIE	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/css/shared_responsive.css?v=eghn9DNyCY67&	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/softokn3.dll	100%	Avira URL Cloud	malware	
http://https://community.cloudflare.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/css/shared_global.css?v=2VoZa2M8Wh3k&	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/he	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/main.js?v=yF_q	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/market/	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/msvcp140.dllU	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/my/wishlist/	0%	Avira URL Cloud	safe	
http://https://95.217.240.101	100%	Avira URL Cloud	malware	
http://https://95.217.240.101/freebl3.dlls	100%	Avira URL Cloud	malware	
http://https://95.217.240.101/msvcp140.dll	100%	Avira URL Cloud	malware	
http://https://community.cloudflare.steamstatic.com/public/javascript/global.js?v=PyuRtGtUpR0t&l=englis	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	0%	Avira URL Cloud	safe	
http://https://steamcommunity.co	100%	Avira URL Cloud	phishing	
http://https://steamcommunity.com/discussions/	0%	Avira URL Cloud	safe	
http://https://community.cloudflare.steamstatic.com/public/css/applications/community/main.css?v=5CgcHEsWGA	0%	Avira URL Cloud	safe	
http://https://t.me/k0mono	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/profiles/76561199686524322/badges	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/profiles/76561199686524322/inventory/	100%	Avira URL Cloud	malware	
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/profilev2.css?v=gNE3gksLVEVa&l=en	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/workshop/	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/mozglue.dll	100%	Avira URL Cloud	malware	
http://https://95.217.240.101/softokn3.dllK	100%	Avira URL Cloud	malware	
http://https://community.cloudflare.steamstatic.com/public/css/globalv2.css?v=pwVclAtHNXwg&l=english&am	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/sqlx.dll	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/profiles/76561199686524322	100%	Avira URL Cloud	malware	
http://https://95.217.240.101/v	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
steamcommunity.com	23.194.234.100	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://95.217.240.101/nss3.dll	true	• Avira URL Cloud: malware	unknown
https://95.217.240.101/freebl3.dll	true	• Avira URL Cloud: malware	unknown
http://https://95.217.240.101/softokn3.dll	false	• Avira URL Cloud: malware	unknown
http://https://95.217.240.101/msvcp140.dll	false	• Avira URL Cloud: malware	unknown
http://https://95.217.240.101/mozglue.dll	false	• Avira URL Cloud: malware	unknown
http://https://95.217.240.101/sqlx.dll	false	• Avira URL Cloud: malware	unknown
https://steamcommunity.com/profiles/76561199686524322	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	JEGHDA.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	JEGHDA.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/tooltip.j	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/?subsection=broadcasts	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://95.217.240.101/nss3.dll2	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/webui/clientcom.js?v=dERfFkkJ-bKK&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/shared_global.js?v=wJD9maDpDcV	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://bridge.lga1.admarketplace.net/ctp?version=16.0.0&key=1696332238301000001.2&ci=1696332238417.	RegAsm.exe, 00000003.00000002.2039843290.0000000000FDF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000FE5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000001068000.00000004.00000020.00020000.00000000.sdmp, IIDHJD.3.dr	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=engli	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/promo/stickers.js?v=GfA42_x2_aub&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpE	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://www.valvesoftware.com/legal.htm	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	RegAsm.exe, 00000003.00000002.2039421679.0000000000572000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://imp.mt48.net/static?id=7RHzfOIXjFEYsBdvlpkX4QqmfZfYfQfafZbXfpbWfpbX7ReNxR3UIG8zInwYIFIVs9eYi	IIDHJD.3.dr	false	• URL Reputation: safe	unknown
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://www.amazon.com/?tag=admarketus-20&ref=pd_sl_7548d4575af019e4c148ccf1a78112802e66a0816a72fc94	RegAsm.exe, 00000003.00000002.2039843290.0000000000FDF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000FE5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000001068000.00000004.00000020.00020000.00000000.sdmp, IIDHJD.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/modalContent.js?v=Wd0kCESeJquW&l=	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://www.mozilla.com/en-US/blocklist/	RegAsm.exe, RegAsm.exe, 00000003.00000002.2047049118.000000006C73D000.00000002.00000001.01000000.00000008.sdmp, mozglue[1].dll.3.dr, mozglue.dll.3.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mozilla.org0/	nss3[1].dll.3.dr, softokn3[1].dll.3.dr, softokn3.dll.3.dr, mozglue[1].dll.3.dr, freebl3[1].dll.3.dr, nss3.dll.3.dr, mozglue.dll.3.dr, freebl3.dll.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101KJE	RegAsm.exe, 00000003.00000002.2039421679.0000000000572000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199686524322	76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/css/shared_responsive.css?v=eghn9DNyCY67&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/points/shop/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/login	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	JEGHDA.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://bridge.lga1.ap01.net/ctp?version=16.0.0&key=1696332238301000001.1&ci=1696332238417.12791&cta	RegAsm.exe, 00000003.00000002.2039843290.0000000000FDF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000FE5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000001068000.00000004.00000020.00020000.00000000.sdmp, IIDHJD.3.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	RegAsm.exe, 00000003.00000002.2039421679.0000000000572000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039421679.000000000060B000.00000040.00000400.00020000.00000000.sdmp, GDAAKF.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/css/promo/summer2017/stickers.css?v=bZKSp7oNwVPK	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	JEGHDA.3.dr	false	• URL Reputation: safe	unknown
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	GCBFBG.3.dr	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101FIE	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

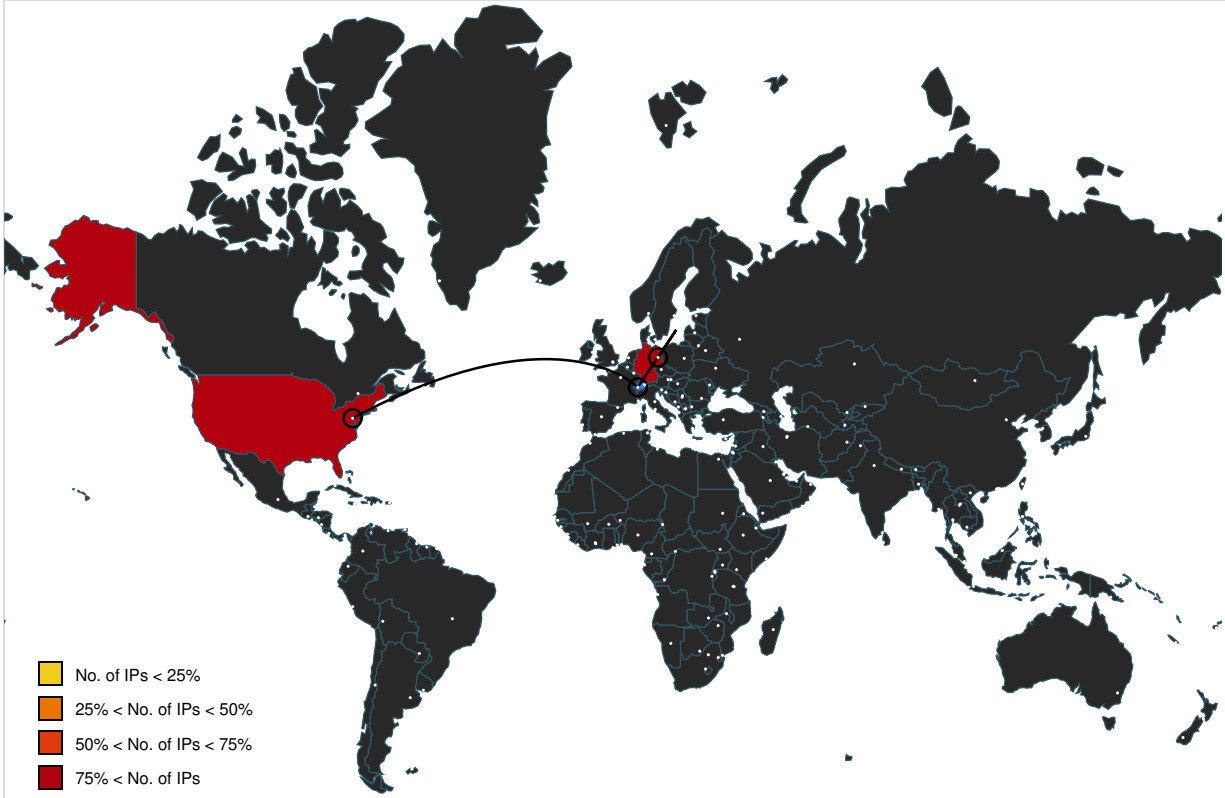
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.cloudflare.steamstatic.com/public/shared/css/shared_global.css?v=2VoZa2M8Wh3k&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/he	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/libraries~b28b	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/header_logo.png	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	GDAAKF.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/main.js?v=yF_q	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/about/	76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/my/wishlist/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	GCBFBG.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC&	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101/msvcp140.dllU	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://95.217.240.101/freebl3.dlls	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://help.steampowered.com/en/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/market/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/news/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101	76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.cloudflare.steamstatic.com/public/javascript/global.js?v=PyuRtGtUpR0t&l=englis	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	JEGHDA.3.dr	false	• URL Reputation: safe	unknown
http://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/manifest.js?v=	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	RegAsm.exe, 00000003.00000002.2039421679.0000000000572000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039421679.000000000060B000.00000040.00000400.00020000.00000000.sdmp, GDAAKF.3.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.co	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp	true	• Sophos S4: illegal phishing domain • Avira URL Cloud: phishing	unknown
http://https://steamcommunity.com/discussions/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/css/applications/community/main.css?v=5CgcHEsWGA	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/stats/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0&	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/steam_refunds/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/images/skin_1/arrowDn9x5.gif	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	GDAAKF.3.dr	false	• URL Reputation: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	JEGHDA.3.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.p	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://t.me/k0mono	file.exe, 00000000.00000002.1589701895.000000000070A000.00000004.00000001.01000000.00000003.sdmp, RegAsm.exe, RegAsm.exe, 00000003.00000002.2039421679.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/profiles/76561199686524322/inventory/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/profiles/76561199686524322/badges	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/workshop/	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/legal/	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000003.00000002.2044042072.000000001928D000.00000002.00001000.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2040755834.00000000132E9000.00000004.00000020.00020000.00000000.sdmp, sqlx[1].dll.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/css/buttons.css?v=tuNiaSwXwcYT&l=engl	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/css/motiva_sans.css?v=GfSjbGKcNYaQ&l=	76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/profilev2.css?v=gNE3gksLVEVa&l=en	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://contile-images.services.mozilla.com/0TegrVVRalreHILhR2WvtD_CFzj13HCDcLqqpvXSOuY.10862.jpg	RegAsm.exe, 00000003.00000002.2039843290.0000000000FDF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000FE5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000001068000.00000004.00000020.00020000.00000000.sdmp, IIDHJD.3.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	JEGHDA.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://95.217.240.101/softokn3.dllK	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.cloudflare.steamstatic.com/public/css/globalv2.css?v=pwVclAtHNXwg&l=english&am	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/header.css?v=vh4BMeDcNiCU&l=engli	RegAsm.exe, 00000003.00000002.2039421679.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.steampowered.com/	76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016ost.exe	RegAsm.exe, 00000003.00000002.2039421679.0000000000572000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	JEGHDA.3.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101/v	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.cloudflare.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	RegAsm.exe, 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.3.dr	false	• URL Reputation: safe	unknown
http://https://avatars.cloudflare.steamstatic.com/fef49e7fa7e1997310d705b2a6158ff8dc1cdfeb_full.jpg	76561199686524322[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://contile-images.services.mozilla.com/obgoOYObjIFea_bXuT6L4LbBJ8j425AD87S1HMD3BWg.9991.jpg	RegAsm.exe, 00000003.00000002.2039843290.0000000000FDF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000000FE5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2039843290.0000000001068000.00000004.00000020.00020000.00000000.sdmp, IIDHJD.3.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.194.234.100	steamcommunity.com	United States		16625	AKAMAI-ASUS	true
95.217.240.101	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1442218
Start date and time:	2024-05-15 20:35:06 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 29s

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:	10
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@11/25@1/2
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • 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.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
20:35:57	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\GHIJJEGDBFII\AEHDAK

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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\GHIJJEGDBFII\CBFIJE

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, cookie 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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j.....}..}..... ....

C:\ProgramData\GHIJJEGDBFII\CBFIJE-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\GHIJJEGDBFII\CFHCGH

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\GHIJJEGDBFII\GCBFBG

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
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\GHIJJEGDBFII\GCBFBG-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\GHIJJEGDBFII\GDAAKF

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 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UlYysX0lxQzh/tsVL:8Ys3QMmRtH+bF+Ul3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j.....

C:\ProgramData\GHIJJEGDBFII\GHIJJE

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
Preview:	SQLite format 3.....@ .....O}.....

C:\ProgramData\GHIJJEGDBFII\HDAFII

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:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7YItnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621(3
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$.....

C:\ProgramData\GHIJJEGDBFII\IIDHJD

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\GHIJJEGDBFII\JEGHDA

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:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

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

C:\ProgramData\GHIJJEGDBFII\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%
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\GHIJJEGDBFII\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%
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\GHIJJEGDBFII\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%
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\GHIJJEGDBFII\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%
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.....@..@.data.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B.....

C:\ProgramData\GHIJJEGDBFII\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:	3A7C260646315CF8C01F44B2EC60974017496BD0D80DD055C7E43B707CADBA2D63AAB5E0EFD435670AA77886ED86368390D42C4017FC433C3C4B9D1C47D0F36
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\76561199686524322[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 (3041), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	35643
Entropy (8bit):	5.382912586977827
Encrypted:	false
SSDEEP:	768:s7pqLtWYmwt5D0gqVUiNGAZPzzgiJmDzJtxvrfukPco1AUmPzzgiJmDzJtxvJ2SC:s78LtWYmwt5D0gqVUcZPzzgiJmDzJtxW
MD5:	7BCE059CFD60B798CB45C3F4C80B9F6C
SHA1:	736FAB76D920E9A5E4BAB9E12E8C85C9D4B22A06
SHA-256:	317AB49AEA660F5D325951C5EF280A54F6192D3B31A15B0F985EA292ED159980
SHA-512:	B0875CD2B58367D1165D373600CE208B63C4E435A62C237729BB66645A43FC5A6DF16CC646553F97700FA5A7E4C3A5EEE4C7591D7A29E8F87662B815E8A5675
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 :: r8p- https://95.217.240.101|</title>...<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">.....<link href="https://community.cloudflare.steamstatic.com/public/shared/css/motiva_sans.css?v=GfSjbGKcNYaQ&l=english&_cdn=cloudflare" rel="stylesheet" type="text/css" >.<link href="https://community.cloudflare.steamstatic.com/public/shared/css/buttons.css?v=tuNiaSwXwcYT&l=english&_cdn=cloudflare" rel="stylesheet" type="text/css" >.<link href="https://community.cloudflare.steamstatic.com/public/shared/css/shared_global.css?v=2VoZa2M8Wh3k&l=english&_cdn=cloudflare" rel="stylesheet" type="text/css" >.<link href="https://community.cloudflare.steamstatic.com/public/css/globalv2.c

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 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B 40
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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%
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:	DD9FF4E06B00DC831439BAB11C10E9B2AE864EA6E780D3835EA7468818F35439F352EF137DA111EFCDF2BB6465F6CA486719451BF6CF32C6A4420A56B1D6457 1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....`.....p.....I- ...@A.... .....&.....@....P..x.....P/..`..\.....\....&..@.....text..... ..`.rdata..I.....@..@.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%
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
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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):	7.529756734354945
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:	382'976 bytes
MD5:	b580ff2d001291bf58bdd23a058ef21b
SHA1:	5013dc6e38bd9d1cbe2f7fc0d983b6812f3f2351
SHA256:	80994b791b545ba6a8c906e046ab6ae79c5875a4f42da07085113b4b6f22f8ca
SHA512:	85643ff028ffa0d7c6e7b3dd69c9316aed5e6c15c364bfdb14ec65ca9859ee8fb2ae04e3990c2275671da27abb727a9505f2acf5453a4bb1a3f4df0664df603b
SSDEEP:	6144:3hp+scz0+j/2LXudxnOqC3dFxYkBY8EdltIPaiTeUkHjUP6PiLNwETfeuBMbxFr9:3SscQu/CLtF3BY87PFi7HJAwETfhMlF5
TLSH:	6684E051B4C1C032D433153A49F4DBB85E7EB9600AA69A9FBB940F7F4F312C1D621A6B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3UT.w4:.w4:.w4:..F9. {4:..F?..4:..F>.b4:...>.e4:...9.b4:..F;.~4:.w4;..4:...?.!4:...3.v4:...8.v4:.Richw4:.....PE..L..

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x4072d9
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:	0x6644F62C [Wed May 15 17:51:40 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:	81b834f6f9db0b945bd836f537996a1f

Entrypoint Preview
Instruction
call 00007F13E0BBF083h
jmp 00007F13E0BBE759h
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007F13E0BBE8FBh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007F13E0BBE8ECh
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007F13E0BBE8EEh
add edx, 28h
cmp edx, esi
jne 00007F13E0BBE8CCh
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007F13E0BBE8DBh
push esi
call 00007F13E0BBF35Dh
test eax, eax
je 00007F13E0BBE902h
mov eax, dword ptr fs:[00000018h]
mov esi, 0045DB4Ch
mov edx, dword ptr [eax+04h]
jmp 00007F13E0BBE8E6h
cmp edx, eax
je 00007F13E0BBE8F2h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007F13E0BBE8D2h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+08h], 00000000h
jne 00007F13E0BBE8E9h
mov byte ptr [0045DB50h], 00000001h

Instruction
call 00007F13E0BBEBA7h
call 00007F13E0BC18F0h
test al, al
jne 00007F13E0BBE8E6h
xor al, al
pop ebp
ret
call 00007F13E0BC92C9h
test al, al
jne 00007F13E0BBE8ECh
push 00000000h
call 00007F13E0BC18F7h
pop ecx
jmp 00007F13E0BBE8CBh
mov al, 01h
pop ebp
ret
push ebp
mov ebp, esp
cmp byte ptr [0045DB51h], 00000000h
je 00007F13E0BBE8E6h
mov al, 01h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x291c8	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5f000	0x1d14	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x27280	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x271c0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x20000	0x174	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

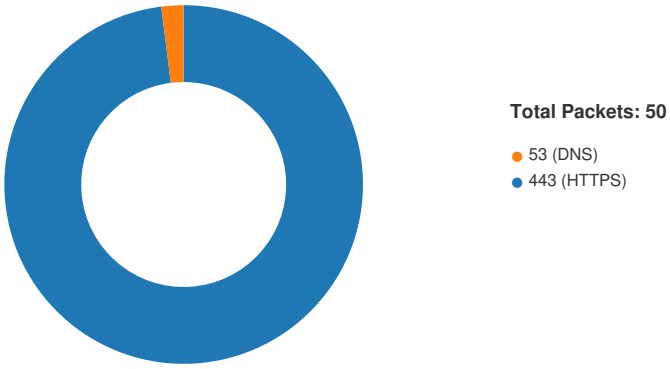
Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1e2ab	0x1e400	6aaddd29a7b1d14c04fafe4373874165	False	0.5765996255165289	data	6.591179392915493	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x20000	0x9a58	0x9c00	c0d3af8d875e80d0742331423512f2ce	False	0.3869941907051282	data	4.658571126756863	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2a000	0x34654	0x33600	2cb86b6c8671c22ce21f5d03dfb1e373	False	0.9822270377128953	data	7.9818411522888875	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x5f000	0x1d14	0x1e00	45d81991a944a5e251cf5f207dbbc2a5	False	0.7373697916666667	data	6.468270351939864	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
GDI32.dll	GetClipBox
USER32.dll	PostQuitMessage
ADVAPI32.dll	CryptDecrypt
KERNEL32.dll	HeapSize, CreateFileW, VirtualAlloc, WaitForSingleObject, GetModuleHandleA, FreeConsole, CreateThread, GetProcAddress, MultiByteToWideChar, GetStringTypeW, WideCharToMultiByte, GetCurrentThreadId, CloseHandle, WaitForSingleObjectEx, GetExitCodeThread, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, EncodePointer, DecodePointer, LCMapStringEx, ReleaseSRWLockExclusive, WakeAllConditionVariable, QueryPerformanceCounter, GetSystemTimeAsFileTime, GetModuleHandleW, GetCPInfo, IsProcessorFeaturePresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, GetCurrentProcessId, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetProcessHeap, RaiseException, RtlUnwind, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, ExitThread, FreeLibraryAndExitThread, GetModuleHandleExW, GetStdHandle, WriteFile, GetModuleFileNameW, ExitProcess, GetCommandLineA, GetCommandLineW, HeapAlloc, HeapFree, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetFileType, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, SetStdHandle, WriteConsoleW

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2024 20:35:50.127605915 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:50.127636909 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:50.127707005 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:50.134161949 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:50.134172916 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:50.364038944 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:50.364135981 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:50.455997944 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:50.456013918 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:50.456284046 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:50.456331968 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:50.461704016 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:50.508116961 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.061505079 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.061527967 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.061563015 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.061635971 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:51.061645985 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.061687946 CEST	49730	443	192.168.2.4	23.194.234.100

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2024 20:35:51.168766975 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.168817997 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.168853998 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:51.168865919 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.168914080 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:51.192764997 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.192811966 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.192836046 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.192854881 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:51.192898989 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:51.208177090 CEST	49730	443	192.168.2.4	23.194.234.100
May 15, 2024 20:35:51.208195925 CEST	443	49730	23.194.234.100	192.168.2.4
May 15, 2024 20:35:51.225543976 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:51.225575924 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:51.225739956 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:51.226167917 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:51.226177931 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:51.967655897 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:51.967739105 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:51.972084999 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:51.972090960 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:51.972296953 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:51.972352028 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:51.972640991 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:52.020127058 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:52.523298979 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:52.523364067 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:52.523390055 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:52.523421049 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:52.528031111 CEST	49731	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:52.528048038 CEST	443	49731	95.217.240.101	192.168.2.4
May 15, 2024 20:35:52.530442953 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:52.530478954 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:52.530564070 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:52.530831099 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:52.530847073 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.003607035 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.003669977 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.004223108 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.004229069 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.006026030 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.006031990 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.896611929 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.896672964 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.896709919 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.896873951 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.896941900 CEST	49732	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.896955013 CEST	443	49732	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.898546934 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.898566961 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:53.898648977 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.898866892 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:53.898880005 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:54.364252090 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:54.364336014 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:54.365077019 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:54.365082979 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:54.366694927 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:54.366699934 CEST	443	49733	95.217.240.101	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2024 20:35:55.240196943 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.240227938 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.240287066 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.240338087 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.240365982 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.240637064 CEST	49733	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.240654945 CEST	443	49733	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.242537022 CEST	49734	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.242563009 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.242651939 CEST	49734	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.242862940 CEST	49734	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.242872000 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.708503008 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.708595037 CEST	49734	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.709259033 CEST	49734	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.709264040 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:55.711061001 CEST	49734	443	192.168.2.4	95.217.240.101
May 15, 2024 20:35:55.711065054 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:56.579741955 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:56.579775095 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:56.579838991 CEST	443	49734	95.217.240.101	192.168.2.4
May 15, 2024 20:35:56.579965115 CEST	49734	443	192.168.2.4	95.217.240.101

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2024 20:35:50.009427071 CEST	58223	53	192.168.2.4	1.1.1.1
May 15, 2024 20:35:50.120599031 CEST	53	58223	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 15, 2024 20:35:50.009427071 CEST	192.168.2.4	1.1.1.1	0xbd2	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false

DNS Answers

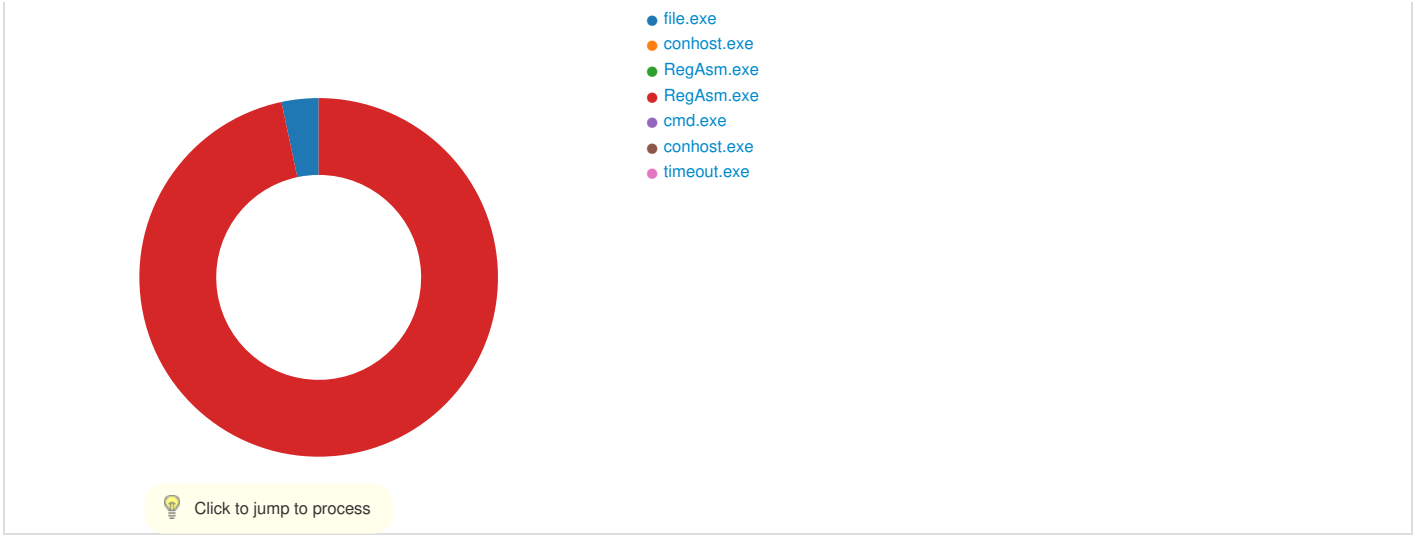
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 15, 2024 20:35:50.120599031 CEST	1.1.1.1	192.168.2.4	0xbd2	No error (0)	steamcommunity.com		23.194.234.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com
- 95.217.240.101

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **6856**, Parent PID: **2580**

General

Target ID:	0
Start time:	20:35:49
Start date:	15/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x6e0000
File size:	382'976 bytes
MD5 hash:	B580FF2D001291BF58BDD23A058EF21B
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: 00000000.00000002.1589701895.000000000070A000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: **6860**, Parent PID: **6856**

General

Target ID:	1
Start time:	20:35:49
Start date:	15/05/2024
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: 3272, Parent PID: 6856

General

Target ID:	2
Start time:	20:35:49
Start date:	15/05/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
Imagebase:	0x4e0000
File size:	65'440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: RegAsm.exe PID: 5984, Parent PID: 6856

General

Target ID:	3
Start time:	20:35:49
Start date:	15/05/2024
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:	0x910000
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: 00000003.00000002.2039421679.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000003.00000002.2039421679.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.2039421679.0000000000572000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000003.00000002.2039843290.0000000000EF1000.00000004.00000020.00020000.00000000.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\GHIJJEGDBFII	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	416B5B	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	405034	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	405034	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	405034	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	405034	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	405034	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	405034	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	405034	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	405034	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	405034	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	405034	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	405034	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	405034	HttpSendRequestA
C:\ProgramData\GHIJJEGDBFII\HDAFII	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	4068AE	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\GDAAKF	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	40D1D9	CopyFileA
C:\ProgramData\GHIJJEGDBFII\CBFIJE	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	40C37E	CopyFileA
C:\ProgramData\GHIJJEGDBFII\JEGHDA	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	40CF40	CopyFileA
C:\ProgramData\GHIJJEGDBFII\AEHDAK	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	40D1D9	CopyFileA
C:\ProgramData\GHIJJEGDBFII\GHIJJE	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	40C37E	CopyFileA
C:\ProgramData\GHIJJEGDBFII\CFHCGH	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	40CF40	CopyFileA
C:\ProgramData\GHIJJEGDBFII\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\GHIJJEGDBFII\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\GHIJJEGDBFII\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\GHIJJEGDBFII\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\GHIJJEGDBFII\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\GHIJJEGDBFII\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\GHIJJEGDBFII\CBFIJE	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	408847	CopyFileA
C:\ProgramData\GHIJJEGDBFII\CBFIJE-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	19054EE7	CreateFileW
C:\ProgramData\GHIJJEGDBFII\CBFIJE-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	19054EE7	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\GCBFBG	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	409223	CopyFileA
C:\ProgramData\GHIJJEGDBFII\GCBFBG-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	19054EE7	CreateFileW
C:\ProgramData\GHIJJEGDBFII\GCBFBG-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	19054EE7	CreateFileW
C:\ProgramData\GHIJJEGDBFII\IIDHJD	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	40B6CC	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\HDAFII	success or wait	1	406DC5	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\GDAAKF	success or wait	1	40D2CF	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\CBFIJE	success or wait	1	40C61C	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\JEGHDA	success or wait	1	40D0C0	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\AEHDAK	success or wait	1	40D2CF	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\GHIJJE	success or wait	1	40C61C	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\CFHCGH	success or wait	1	40D0C0	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\CBFIJE-shm	success or wait	1	19055612	DeleteFileW
C:\ProgramData\GHIJJEGDBFII\CBFIJE-wal	success or wait	1	19055612	DeleteFileW
C:\ProgramData\GHIJJEGDBFII\CBFIJE	success or wait	1	408CAA	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\GCBFBG-shm	success or wait	1	19055612	DeleteFileW
C:\ProgramData\GHIJJEGDBFII\GCBFBG-wal	success or wait	1	19055612	DeleteFileW
C:\ProgramData\GHIJJEGDBFII\GCBFBG	success or wait	1	409480	DeleteFileA
C:\ProgramData\GHIJJEGDBFII\IIDHJD	success or wait	1	40B7A1	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199686524322[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"><link	success or wait	16	4050D8	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 00	MZ@!L!This program cannot be run in DOS mode.$7ZYZYZYZnY\Y]Y XYYZXYO\EYO]UYOZLYl3][Yl3Y[Yl3[Yl3[[YRichZY	success or wait	2254	40433D	InternetReadFile
C:\ProgramData\GHIJJEGDBFII\HDAFII	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0b 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	4068AE	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\GDAAKF	0	131072	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 04 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 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 04 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 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	SQLite format 3@ ' .j	success or wait	2	40D1D9	CopyFileA
C:\ProgramData\GHIJJEGDBFII\CBFIJE	0	40960	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 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	1	40C37E	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\JEGHDA	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 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	40CF40	CopyFileA
C:\ProgramData\GHIJJEGDBFII\AEHDAK	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	SQLite format 3@ .O}	success or wait	1	40D1D9	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\GHIJJE	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	SQLite format 3@ .O}	success or wait	1	40C37E	CopyFileA
C:\ProgramData\GHIJJEGDBFII\CFHCGH	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	SQLite format 3@ 8$.O}4	success or wait	1	40CF40	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 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.$PEL4c"!4p@AHS	success or wait	631	404ECE	InternetReadFile
C:\ProgramData\GHIJJEGDBFII\freebl3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	670	404EAA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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.$PEL4c"!^j@A`W,	success or wait	542	404ECE	InternetReadFile
C:\ProgramData\GHIJJEGDBFII\mozglue.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	594	404EAA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	413	404ECE	InternetReadFile
C:\ProgramData\GHIJJEGDBFII\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	404EAA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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.$PEL4c"!.`pl-@A&@	success or wait	1875	404ECE	InternetReadFile
C:\ProgramData\GHIJJEGDBFII\nss3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1999	404EAA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 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 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 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.$PEL4c"!PSg@ADvSw	success or wait	237	404ECE	InternetReadFile
C:\ProgramData\GHIJJEGDBFII\softokn3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	252	404EAA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	404ECE	InternetReadFile
C:\ProgramData\GHIJJEGDBFII\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 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	79	404EAA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\CBFIJE	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	SQLite format 3@ .j}}	success or wait	1	408847	CopyFileA
C:\ProgramData\GHIJJEGDBFII\GCBFBG	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	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAsqpqp{ooh nnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	409223	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\GHIJJEGDBFII\IIDHJD	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	40B6CC	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	406206	ReadFile
C:\ProgramData\GHIJJEGDBFII\HDAFII	0	100	success or wait	6	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\GDAAKF	0	100	success or wait	6	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\GDAAKF	0	100	success or wait	6	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\CBFIJE	0	100	success or wait	6	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\JEGHDA	0	100	success or wait	18	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\JEGHDA	0	100	success or wait	9	1904FE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	406206	ReadFile
C:\ProgramData\GHIJJEGDBFII\AEHDAK	0	100	success or wait	6	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\AEHDAK	0	100	success or wait	6	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\GHIJJE	0	100	success or wait	6	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\CFHCGH	0	100	success or wait	10	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\CFHCGH	0	100	success or wait	10	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\CBFIJE	0	100	success or wait	4	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\GCBFBG	0	100	success or wait	5	1904FE09	ReadFile
C:\ProgramData\GHIJJEGDBFII\IIDHJD	0	9571	success or wait	2	406206	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: **2860**, Parent PID: **5984**

General

Target ID:	7
Start time:	20:36:34
Start date:	15/05/2024
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\GHIJJEGDBFII" & exit
Imagebase:	0x7ff72bec0000
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: **3412**, Parent PID: **2860**

General

Target ID:	8
Start time:	20:36:34
Start date:	15/05/2024
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: **2116**, Parent PID: **2860**

General

Target ID:	9
Start time:	20:36:34
Start date:	15/05/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 10
Imagebase:	0xd00000
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