ID: 1443407
Sample Name: file.exe
Cookbook: default.jbs
Time: 18:05:08
Date: 17/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

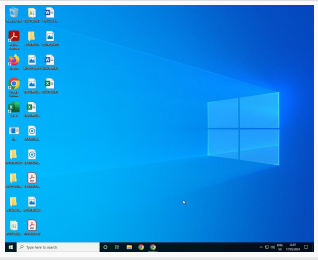
Windows Analysis Report

file.exe

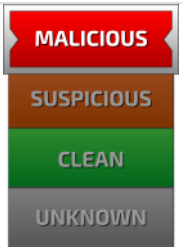
Overview

General Information

Sample name:	file.exe
Analysis ID:	1443407
MD5:	75db6dfdebb9b..
SHA1:	5bc1ceec4269…
SHA256:	a2f94952c89ea..
Tags:	exe
Infos:	



Detection



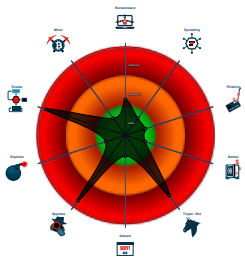
Vidar

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: 6352 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 75DB6DFDEBB9BF0D98ACFC15F2219C62)
  - conhost.exe (PID: 5696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - RegAsm.exe (PID: 1600 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
    - cmd.exe (PID: 7044 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\FCGCGDHJEGHJ" & exit MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 2860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - timeout.exe (PID: 5392 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
00000002.00000002.2640792644.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2640792644.0000000000400000.00000040.00000400.00020000.00000000.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
00000000.00000002.1950868153.0000000000AD8000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: file.exe PID: 6352	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.RegAsm.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x221f0:$s1: JohnDoe • 0x31f80:$s1: JohnDoe • 0x221e8:$s2: HAL9TH
2.2.RegAsm.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.RegAsm.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x20df0:$s1: JohnDoe • 0x20de8:$s2: HAL9TH
0.2.file.exe.ab0000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

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

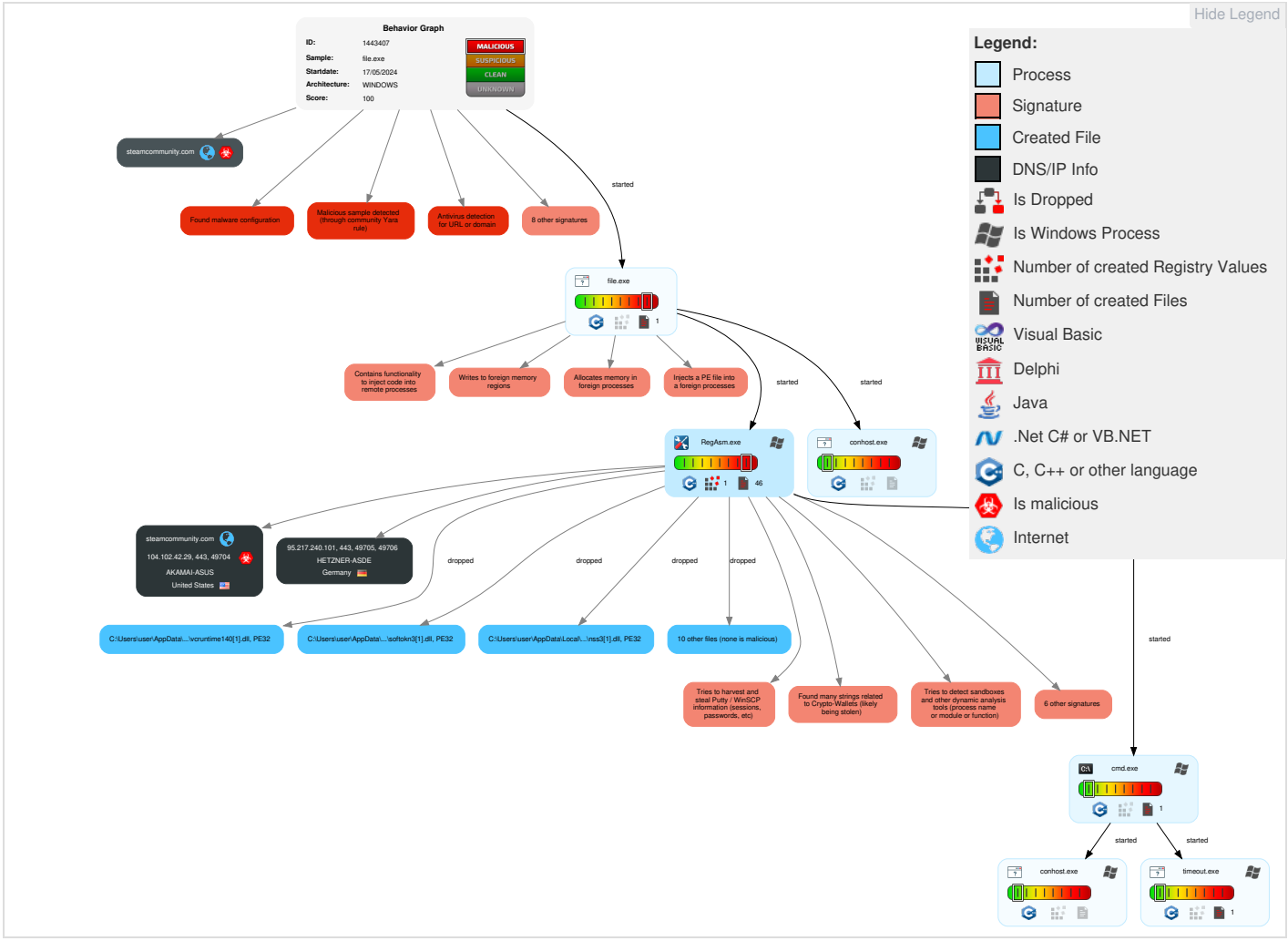
Yara detected Vidar

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	At	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	4 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Masquerading	NTDS	5 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

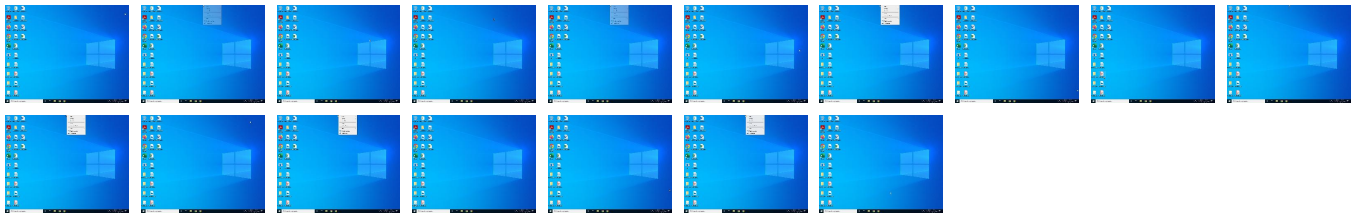
Behavior Graph



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.1352999	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\FCGCGDHJEGHJ\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\FCGCGDHJEGHJ\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\FCGCGDHJEGHJ\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\FCGCGDHJEGHJ\nss3.dll	0%	ReversingLabs		
C:\ProgramData\FCGCGDHJEGHJ\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\FCGCGDHJEGHJ\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\53IVYM2Y\sqlx[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\freebl3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\mozglue[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\msvcp140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\nss3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\softokn3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\vcruntime140[1].dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://store.steampowered.com/subscriber_agreement/	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/libraries~b28b7af6	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/modalContent.js?v=L35TrLJDfqtD&l=engl	0%	URL Reputation	safe	
http://www.valvesoftware.com/legal.htm	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/css/promo/summer2017/stickers.css?v=HA2Yr5oy3FFG&	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.png	0%	URL Reputation	safe	
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/profile.js?v=ly1ies1ROjUT&l=english	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	0%	URL Reputation	safe	
http://www.mozilla.com/en-US/blocklist/	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/css/skin_1/header.css?v=NFoCa4OkAxRb&l=english	0%	URL Reputation	safe	
http://https://mozilla.org0/	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://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://avatars.akamai.steamstatic.com/fef49e7fa7e1997310d705b2a6158ff8dc1cdfeb_full.jpg	0%	URL Reputation	safe	
http://https://store.steampowered.com/privacy_agreement/	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0	0%	URL Reputation	safe	
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.GVegJq3nFfBL	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=english	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_logo.png	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC	0%	URL Reputation	safe	
http://https://store.steampowered.com/about/	0%	URL Reputation	safe	
http://https://help.steampowered.com/en/	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	0%	Avira URL Cloud	safe	
http://https://bridge.sfo1.admarketplace.net/ctp?version=16.0.0&key=169642513640080000.2&ci=1696425136743.	0%	Avira URL Cloud	safe	
http://https://95.217.240.101IDH	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/freebl3.dll	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=6MtR	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/nss3.dll	100%	Avira URL Cloud	malware	
http://https://store.steampowered.com/news/	0%	URL Reputation	safe	
http://https://steamcommunity.com/?subsection=broadcasts	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIlcMzCffX6&	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://https://community.akamai.steamstatic.com/public/javascript/promo/stickers.js?v=upl9NJ5D2xkP&l=en	0%	URL Reputation	safe	
http://https://store.steampowered.com/stats/	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	0%	URL Reputation	safe	
http://https://store.steampowered.com/steam_refunds/	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	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.akamai.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v=pSv	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=engl	0%	URL Reputation	safe	
http://https://95.217.240.101/sqlx.dll	100%	Sophos S4	malware repository uri	
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	0%	Avira URL Cloud	safe	
http://https://store.steampowered.com/	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/images/skin_1/arrowDn9x5.gif	0%	URL Reputation	safe	
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199686524322	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/softokn3.dlleS	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://store.st	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_global.js?v=REEGJU1hwkYl&am	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh	0%	URL Reputation	safe	
http://https://95.217.240.101/softokn3.dll	100%	Avira URL Cloud	malware	
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%2	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/msvcp140.dllsS9	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english	0%	Avira URL Cloud	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	0%	URL Reputation	safe	
http://https://contile-images.services.mozilla.com/obgoOYObjIFea_bXuT6L4LbBJ8j425AD87S1HMD3BWg.9991.jpg	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/shared/css/buttons.css?v=PUJIfhtcQn7W&l=english	0%	URL Reputation	safe	
http://store.steampowered.com/account/cookiepreferences/	0%	URL Reputation	safe	
http://https://store.steampowered.com/mobile	0%	URL Reputation	safe	
http://https://www.bestbuy.com/site/electronics/top-deals/pcmcat1563299784494.c/?id=pcmcat1563299784494&ref	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/freebl3.dllwT=	100%	Avira URL Cloud	malware	
http://https://www.amazon.com/?tag=admarketus-20&ref=pd_sl_35787f1071928bc3a1aef90b79c9bee9c64ba6683fde7477	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/my/wishlist/	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/css/applications/community/main.css?v=5CgcHEsWGAFt&a	0%	Avira URL Cloud	safe	
http://https://95.217.240.101	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/market/	0%	Avira URL Cloud	safe	
http://https://imp.mt48.net/static?id=7RHzfOIXjFEYsBdvlpkX4Qqm4p8dfCfm4pbW1pbWfpbW7ReNxR3UIG8zInwYIFIVs9eYi	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/msvcp140.dll	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/tIP	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/D	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/discussions/	0%	Avira URL Cloud	safe	
http://https://t.me/k0mono	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/workshop/	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/profiles/76561199686524322/inventory/	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/profiles/76561199686524322/badges	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://95.217.240.101/O	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&l=e	0%	Avira URL Cloud	safe	
http://https://95.217.240.101KEG	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/javascript/webui/clientcom.js?v=L3Ed_Gybseku&l=e	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/main.js?v=soQOTmUz	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/sqlx.dll	100%	Avira URL Cloud	malware	
http://https://95.217.240.101/mozglue.dll	100%	Avira URL Cloud	malware	
http://https://95.217.240.101/sqlx.dlll	100%	Avira URL Cloud	malware	
http://https://bridge.sfo1.ap01.net/ctp?version=16.0.0&key=1696425136400800000.1&ci=1696425136743.12791&cta	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/profiles/76561199686524322	100%	Avira URL Cloud	malware	
http://https://contile-images.services.mozilla.com/u1AuJcj32cbVUf9NjMipLXEYwu2uFlt4lsj-ccwVqEs.36904.jpg	0%	Avira URL Cloud	safe	
http://https://95.217.240.101/msvcp140.dllyS#	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
steamcommunity.com	104.102.42.29	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
https://95.217.240.101/softokn3.dll	true	• 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
https://95.217.240.101/sqlx.dll	true	• Sophos S4: malware repository uri • Avira URL Cloud: malware	unknown
https://steamcommunity.com/profiles/76561199686524322	true	• Avira URL Cloud: malware	unknown
http://https://95.217.240.101/vcruntime140.dll	false	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	HIEBAK.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	HIEBAK.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/?subsection=broadcasts	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bridge.sfo1.admarketplace.net/ctp?version=16.0.0&key=1696425136400800000.2&ci=1696425136743.	RegAsm.exe, 00000002.00000002.2641871501.0000000000F67000.00000004.00000020.00020000.00000000.sdmp, GCGDGH.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/libraries~b28b7af6	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/javascript/modalContent.js?v=L35TrLJDfqtD&l=engl	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://www.valvesoftware.com/legal.htm	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101IDH	RegAsm.exe, 00000002.00000002.2640792644.0000000000572000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/promo/summer2017/stickers.css?v=HA2Yr5oy3FFG&	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=6MtR	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.png	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIIcMzCffX6&	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/profile.js?v=Iy1ies1ROjUT&l=english	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://www.mozilla.com/en-US/blocklist/	RegAsm.exe, RegAsm.exe, 00000002.00000002.2650409954.000000006C82D000.00000002.00000001.01000000.00000008.sdmp, mozglue[1].dll.2.dr, mozglue.dll.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/skin_1/header.css?v=NFoCa4OkAxRb&l=english	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown

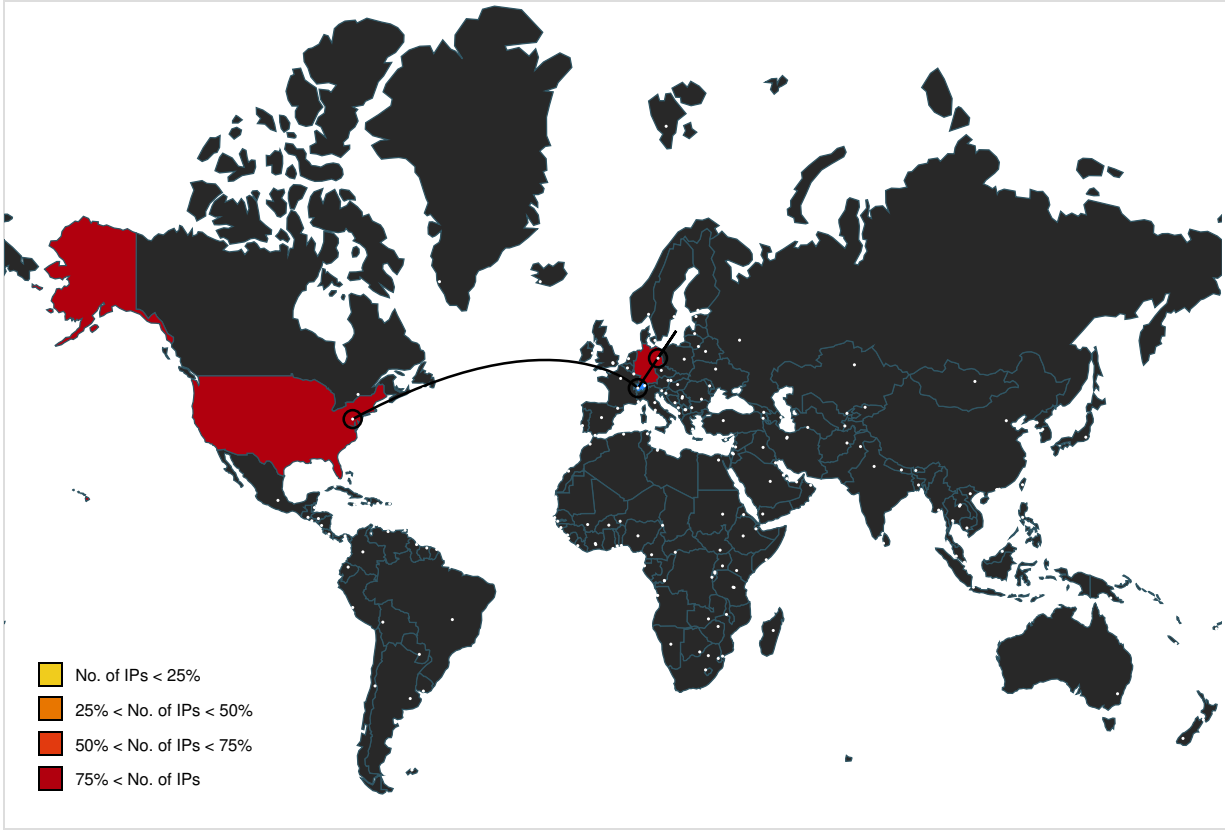
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mozilla.org0/	freebl3.dll.2.dr, nss3[1].dll.2.dr, softokn3[1].dll.2.dr, softokn3.dll.2.dr, mozglue[1].dll.2.dr, mozglue.dll.2.dr, nss3.dll.2.dr, freebl3[1].dll.2.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199686524322	76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%2	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101/softokn3.dlleS	RegAsm.exe, 00000002.00000002.2641871501.0000000000F43000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://store.st	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/points/shop/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	HIEBAK.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	HIEBAK.2.dr	false	• URL Reputation: safe	unknown
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	KJKJJJ.2.dr	false	• URL Reputation: safe	unknown
http://https://avatars.akamai.steamstatic.com/fef49e7fa7e1997310d705b2a6158ff8dc1cdfeb_full.jpg	76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101/msvcp140.dllsS9	RegAsm.exe, 00000002.00000002.2641871501.0000000000F43000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_global.js?v=REEGJU1hwkYI&am	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.GVegJq3nFfBL	KJKJJJ.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.bestbuy.com/site/electronics/top-deals/pcmcat1563299784494.c/?id=pcmcat1563299784494&ref	RegAsm.exe, 00000002.00000002.2641871501.0000000000F67000.00000004.00000020.00020000.00000000.sdmp, GCGDGH.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://95.217.240.101/freebl3.dllwT=	RegAsm.exe, 00000002.00000002.2641871501.0000000000F43000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=english	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://www.amazon.com/?tag=admarketus-20&ref=pd_sl_35787f1071928bc3a1aef90b79c9bee9c64ba6683fde7477	RegAsm.exe, 00000002.00000002.2641871501.0000000000F67000.00000004.00000020.00020000.00000000.sdmp, GCGDGH.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_logo.png	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/about/	76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/my/wishlist/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.steampowered.com/en/	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/market/	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/news/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://imp.mt48.net/static?id=7RHzfOIXjFEYsBdvlpkX4Qqm4p8dfCfm4pbW1pbWfpbW7ReNxR3UIG8zInwYIFIVs9eYi	GCGDGH.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://95.217.240.101	76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/css/applications/community/main.css?v=5CgcHEsWGAFt&a	RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/tIP	RegAsm.exe, 00000002.00000002.2641871501.0000000000EC2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	HIEBAK.2.dr	false	• URL Reputation: safe	unknown
http://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/promo/stickers.js?v=upl9NJ5D2xkP&l=en	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/discussions/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/stats/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.steampowered.com/steam_refunds/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	HIEBAK.2.dr	false	• URL Reputation: safe	unknown
http://https://t.me/k0mono	file.exe, 00000000.00000002.1950868153.000000000AD8000.00000004.00000001.01000000.00000003.sdmp, RegAsm.exe, RegAsm.exe, 00000002.00000002.2640792644.000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://95.217.240.101/D	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/profiles/76561199686524322/inventory/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/profiles/76561199686524322/badges	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/workshop/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://95.217.240.101/O	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://store.steampowered.com/legal/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&l=e	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/webui/clientcom.js?v=L3Ed_Gybseku&l=e	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000002.00000002.2647482481.000000001B6CD000.00000002.00001000.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2643922195.0000000015724000.00000004.00000020.00020000.00000000.sdmp, sqlx[1].dll.2.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101KEG	RegAsm.exe, 00000002.00000002.2640792644.000000000060B000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/main.js?v=soQOTmUz	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v=pSv	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=engl	76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	HIEBAK.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/	76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://bridge.sfo1.ap01.net/ctp?version=16.0.0&key=1696425136400800000.1&ci=1696425136743.12791&cta	RegAsm.exe, 00000002.00000002.2641871501.0000000000F67000.00000004.00000020.00020000.00000000.sdmp, GCGDGH.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/images/skin_1/arrowDn9x5.gif	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	HIEBAK.2.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101/sqlx.dlll	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://contile-images.services.mozilla.com/u1AuJcj32cbVUf9NjMipLXEYwu2uFIt4lsj-ccwVqEs.36904.jpg	RegAsm.exe, 00000002.00000002.2641871501.0000000000F67000.00000004.00000020.00020000.00000000.sdmp, GCGDGH.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://contile-images.services.mozilla.com/obgoOYObjIFea_bXuT6L4LbBJ8j425AD87S1HMD3BWg.9991.jpg	RegAsm.exe, 00000002.00000002.2641871501.0000000000F67000.00000004.00000020.00020000.00000000.sdmp, GCGDGH.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/css/buttons.css?v=PUJIfhtcQn7W&l=english	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://95.217.240.101/msvcp140.dllyS#	RegAsm.exe, 00000002.00000002.2641871501.0000000000F43000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://store.steampowered.com/account/cookiepreferences/	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/mobile	RegAsm.exe, 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2640792644.000000000043C000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.102.42.29	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:	1443407
Start date and time:	2024-05-17 18:05:08 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 7m 1s
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@9/27@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

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.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
12:06:06	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\FCGCGDHJEGHJ\DAKJDA

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 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4

SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0 0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\ProgramData\FCGCGDHJEGHJ\DHDHJJ

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 5, cookie 0x3, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8439810553697228
Encrypted:	false
SSDEEP:	24:TLyAF1kwNbXYFpFNYcw+6UwcQVXH5fBO9p7n52GmCWGf+dyMDCFVE1:TeAFawNLopFgU10XJBOB2Gbf+ba+
MD5:	9D46F142BBCF25D0D495FF1F3A7609D3
SHA1:	629BD8CD800F9D5B078B5779654F7CBFA96D4D4E
SHA-256:	C11B443A512184E82D670BA6F7886E98B03C27CC7A3CEB1D20AD23FCA1DE57DA
SHA-512:	AC90306667AFD38F73F6017543BDBB0B359D79740FA266F587792A94FDD35B54CCE5F6D85D5F6CB7F4344BEDAD9194769ABB3864AAE7D94B4FD6748C31250A0 2
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\ProgramData\FCGCGDHJEGHJ\EBGCBA

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 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j...$.....g..... ....

C:\ProgramData\FCGCGDHJEGHJ\EBKJDB

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 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47 A
Malicious:	false

Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\ProgramData\FCGCGDHJEGHJ\FCGCGD	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\ProgramData\FCGCGDHJEGHJ\GCGDGH	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with very long lines (1743), with CRLF line terminators
Category:	dropped
Size (bytes):	9504
Entropy (8bit):	5.512408163813622
Encrypted:	false
SSDEEP:	192:nnPOeRnWYbBp6RJ0aX+H6SEXKxkHWNBw8D4Sl:PeegJUaJHEw90
MD5:	1191AEB8EAFD5B2D5C29DF9B62C45278
SHA1:	584A8B78810AEE6008839EF3F1AC21FD5435B990
SHA-256:	0BF10710C381F5FCF42F9006D252E6CAFD2F18840865804EA93DAA06658F409A
SHA-512:	86FF4292BF8B6433703E4E650B6A4BF12BC203EF4BBBB2BC0EEEA8A3E6CC1967ABF486EEDCE80704D1023C15487CC34B6B319421D73E033D950DBB1724ABA DD5
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", "9e34c6e7-cbed-40a0-ba63-35488e171013");..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", 1696426836);..user_pref("app.update.lastUpdateTime.region-update-timer", 0);..user_pref("app.update.lastUpdateTime.rs-experiment-loader-timer", 1696426837);..user_pref("app.update.lastUpdateTime.xpi-signature-verification

C:\ProgramData\FCGCGDHJEGHJ\HDGIJJ	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\ProgramData\FCGCGDHJEGHJ\HIEBAK

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):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\ProgramData\FCGCGDHJEGHJ\JDGCGD

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 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W.....

C:\ProgramData\FCGCGDHJEGHJ\KJKJJJ

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):	0.03859996294213402
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWHxDSjENbx56p3DisuwAyHI:58r54w0VW3xWdkEFxcp3y/y
MD5:	D2A38A463B7925FE3ABE31ECCCE66ACA
SHA1:	A1824888F9E086439B287DEA497F660F3AA4B397
SHA-256:	474361353F00E89A9ECB246EC4662682392EBAF4F2A4BE9ABB68BBEBE33FA4A0
SHA-512:	62DB46A530D952568EFBFF7796106E860D07754530B724E0392862EF76FDF99043DA9538EC0044323C814DF59802C3BB55454D591362CB9B6E39947D11E981F7
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\FCGCGDHJEGHJ\KJKJJJ-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\FCGCGDHJEGHJ\KKJEBA

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

C:\ProgramData\FCGCGDHJEGHJ\KKJEBA-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\FCGCGDHJEGHJ\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.$..PE..L....4.c....."!.....4.....p.....@A.... .....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F.. .0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..."..... @..B.....

C:\ProgramData\FCGCGDHJEGHJ\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\FCGCGDHJEGHJ\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\FCGCGDHJEGHJ\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\FCGCGDHJEGHJ\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\FCGCGDHJEGHJ\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\53IVYM2Y\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:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E57033
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\PMW3U6MX\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\PMW3U6MX\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\PMW3U6MX\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\PMW3U6MX\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.....l- ...@A.... .....&.....@....P..x.....P/...`..\.....\....&..@.....text..... ..`.rdata..l.....@..@.data...DR.. .....@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\....`.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\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\PMW3U6MX\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:	3A7C260646315CF8C01F44B2EC60974017496BD0D80DD055C7E43B707CADBA2D63AAB5E0EFD435670AA77886ED86368390D42C4017FC433C3C4B9D1C47D0F3 6
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\T9RRWRNL\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 (2969), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	34771
Entropy (8bit):	5.384707329935698
Encrypted:	false
SSDEEP:	768:Ddpqm+0Ih3YAA9CWGA2fcDAZPzzgiJmDzJtxvrfJkPVoEAdmPzzgiJmDzJtxvJ2i:Dd8m+0Ih3YAA9CWGA2FZPzzgiJmDzJtZ
MD5:	E1272A5DEF427D3C572F30E33137E66F
SHA1:	2418DEAEC6C03B7E940B235F5B22DF985BA4E51C
SHA-256:	2E5105A3078B8C83EEA7F86251F0D56C93C6749A5C9ED44A23D06566E9550C24
SHA-512:	508997728F401092B15DA2FFD91A5275A3BEA4AC87E30ED5DD24811D1D2F6F76013F2E9B43FC898420BD326C7F86FC42DDA8BAFD7F4B3BA81C68A3FAC694B48
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.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/buttons.css?v=PUJIfhtcQn7W&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english" rel="stylesheet" type="text/css" >.<link hr

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.559890664251954
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:	372'224 bytes
MD5:	75db6dfdebb9bf0d98acfc15f2219c62
SHA1:	5bc1ceec4269b4e893f2b00c1c4b3c0cb42a3291
SHA256:	a2f94952c89ea440f82877365db5b4a5cf14a10e4168a22a92fce4a8fd98404f
SHA512:	b295c110369cb2c56d87aab45ff93961b076474d16ca9a7138ab3e6e7acbc8a13a2949dcbc88e6f2e96e4fae793e1793b3052c7ec390ee3d6cd517029583dd2f
SSDEEP:	6144:1JhLSp8zWMtAJA0Z9aRlEiw+pVc4Amr7me33k/JNSdiaJIlsZa6n:pLSpmqKRw+84B7mA3aJE4aOAFn
TLSH:	C384D050B0C08031D663253649E0EBB55E3EF9614F619E9F37A80EBF4F342D2DA61A5B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.(./.{./.{./.{*].z./.{*].zS/.{*].z./.{*].z./.{./.{./.{;..z./.{;..z./.{;..z./.{...z./.{...z./.{Rich./.{.....PE..L....fGf...

File Icon

Icon Hash:	00928e8e8686b000

Static PE Info

General

Entrypoint:	0x405cde
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:	0x66476698 [Fri May 17 14:15:52 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:	e0b6966096a2c186c5f52fee6a381e0f

Entrypoint Preview

Instruction
call 00007F3884E7D9DBh
jmp 00007F3884E7D0A9h
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov ecx, dword ptr [ebp-10h]
xor ecx, ebp
call 00007F3884E7CF95h
jmp 00007F3884E7D212h
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [0045A500h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [0045A500h]
xor eax, ebp

Instruction
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [0045A500h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], esp
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x26b54	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5d000	0x1a54	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x250e8	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	0x25028	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1e000	0x15c	.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	0x1c59f	0x1c600	c974584c4e13e2149107eff417dd9cd3	False	0.5786756607929515	data	6.607233236723112	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1e000	0x933e	0x9400	f5b90bf6728e730f08e6ae3125e52278	False	0.39123205236486486	data	4.691228677009398	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x28000	0x3433c	0x33400	c7f65d0fd90704e9d511f9e8abbc9eb8	False	0.9840463033536585	data	7.984832613465078	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

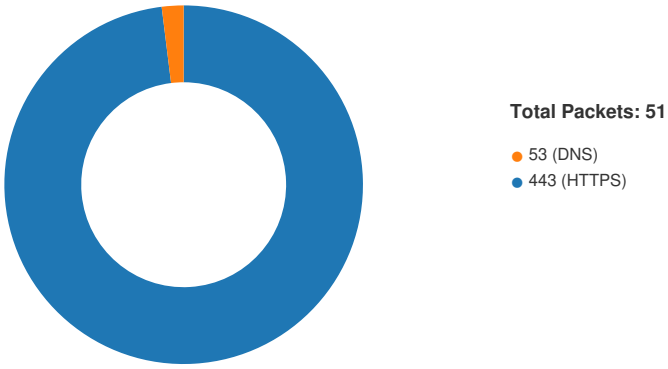
Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x5d000	0x1a54	0x1c00	898c036d1f57c251ff0d1554c59a02d7	False	0.7325613839285714	data	6.391338335451278	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2024 18:05:50.275969982 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:50.276067019 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:50.276166916 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:50.302129984 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:50.302206993 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:51.500148058 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:51.500242949 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:51.735167980 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:51.735254049 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:51.735675097 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:51.735737085 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:51.737740040 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:51.784113884 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.515008926 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.515043974 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.515063047 CEST	443	49704	104.102.42.29	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2024 18:05:52.515149117 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.515212059 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.515264988 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.515264988 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.659703970 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.659733057 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.659960032 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.660023928 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.660087109 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.702033997 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.702147007 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.702244997 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.702244997 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.702744007 CEST	49704	443	192.168.2.5	104.102.42.29
May 17, 2024 18:05:52.702786922 CEST	443	49704	104.102.42.29	192.168.2.5
May 17, 2024 18:05:52.718935966 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:52.718996048 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:52.719536066 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:52.719536066 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:52.719594002 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:54.403044939 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:54.403175116 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:54.413886070 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:54.413906097 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:54.414103031 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:54.414161921 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:54.414673090 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:54.456116915 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:55.392337084 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:55.392419100 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:55.392488003 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:55.392488003 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:55.395876884 CEST	49705	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:55.395894051 CEST	443	49705	95.217.240.101	192.168.2.5
May 17, 2024 18:05:55.398233891 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:55.398318052 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:55.398417950 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:55.398650885 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:55.398685932 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:56.921423912 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:56.921662092 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:56.922190905 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:56.922218084 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:56.923963070 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:56.923975945 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:58.233835936 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:58.233923912 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:58.233968019 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:58.234036922 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:58.234335899 CEST	49706	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:58.234360933 CEST	443	49706	95.217.240.101	192.168.2.5
May 17, 2024 18:05:58.236429930 CEST	49707	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:58.236515999 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:05:58.236618996 CEST	49707	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:58.236922979 CEST	49707	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:58.236948013 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:05:59.803332090 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:05:59.803555965 CEST	49707	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:59.804317951 CEST	49707	443	192.168.2.5	95.217.240.101

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2024 18:05:59.804347038 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:05:59.805931091 CEST	49707	443	192.168.2.5	95.217.240.101
May 17, 2024 18:05:59.805943012 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:06:01.131469965 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:06:01.131491899 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:06:01.131537914 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:06:01.131748915 CEST	49707	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:01.131985903 CEST	49707	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:01.132009029 CEST	443	49707	95.217.240.101	192.168.2.5
May 17, 2024 18:06:01.133892059 CEST	49708	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:01.133915901 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:01.134006023 CEST	49708	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:01.134257078 CEST	49708	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:01.134263992 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:02.658077002 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:02.658169031 CEST	49708	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:02.658602953 CEST	49708	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:02.658608913 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:02.660201073 CEST	49708	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:02.660206079 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:04.024296999 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:04.024359941 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:04.024411917 CEST	49708	443	192.168.2.5	95.217.240.101
May 17, 2024 18:06:04.024425030 CEST	443	49708	95.217.240.101	192.168.2.5
May 17, 2024 18:06:04.024454117 CEST	49708	443	192.168.2.5	95.217.240.101

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2024 18:05:50.215388060 CEST	65439	53	192.168.2.5	1.1.1.1
May 17, 2024 18:05:50.261188984 CEST	53	65439	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 17, 2024 18:05:50.215388060 CEST	192.168.2.5	1.1.1.1	0xb9dd	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false

DNS Answers

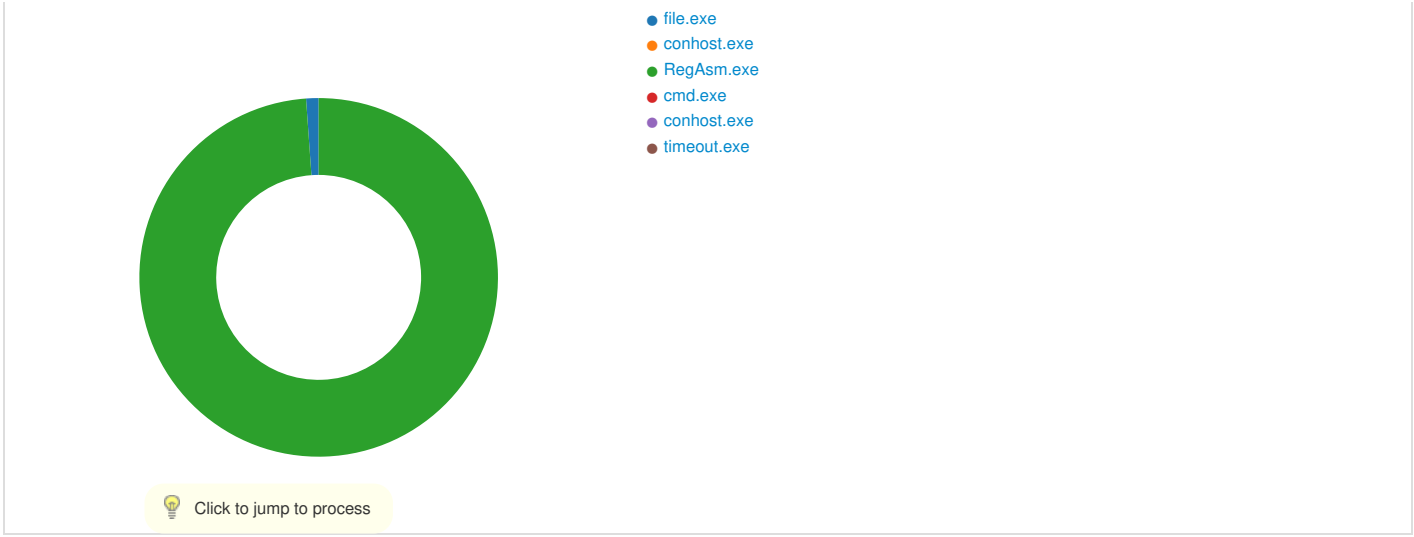
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 17, 2024 18:05:50.261188984 CEST	1.1.1.1	192.168.2.5	0xb9dd	No error (0)	steamcommunity.com		104.102.42.29	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com
- 95.217.240.101

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 6352, Parent PID: 1028

General

Target ID:	0
Start time:	12:05:49
Start date:	17/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0xab0000
File size:	372'224 bytes
MD5 hash:	75DB6DFDEBB9BF0D98ACFC15F2219C62
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: 00000000.00000002.1950868153.0000000000AD8000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: 5696, Parent PID: 6352

General

Target ID:	1
Start time:	12:05:49
Start date:	17/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
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: **1600**, Parent PID: **6352**

General

Target ID:	2
Start time:	12:05:49
Start date:	17/05/2024
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:	0x8c0000
File size:	65'440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000002.00000002.2640792644.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000002.00000002.2640792644.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000002.00000002.2641871501.0000000000EF0000.00000004.00000020.00020000.00000000.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\FCGCGDHJEGHJ	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
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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\FCGCGDHJEGHJ\DHDHJJ	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
C:\ProgramData\FCGCGDHJEGHJ\DAKJDA	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\FCGCGDHJEGHJ\HDGIJJ	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\FCGCGDHJEGHJ\HIEBAK	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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\EBGCBA	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	4068AE	CopyFileA
C:\ProgramData\FCGCGDHJEGHJ\EBKJDB	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\FCGCGDHJEGHJ\FCGCGD	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\FCGCGDHJEGHJ\JDGCGD	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\FCGCGDHJEGHJ\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\FCGCGDHJEGHJ\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\FCGCGDHJEGHJ\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\FCGCGDHJEGHJ\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\FCGCGDHJEGHJ\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\FCGCGDHJEGHJ\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\FCGCGDHJEGHJ\KKJEBA	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\FCGCGDHJEGHJ\KKJEBA-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B494EE7	CreateFileW
C:\ProgramData\FCGCGDHJEGHJ\KKJEBA-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B494EE7	CreateFileW
C:\ProgramData\FCGCGDHJEGHJ\KJKJJJ	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\FCGCGDHJEGHJ\KJKJJJ-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B494EE7	CreateFileW
C:\ProgramData\FCGCGDHJEGHJ\KJKJJJ-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1B494EE7	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\GCGDGH	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\FCGCGDHJEGHJ\DHDHJJ	success or wait	1	406DC5	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\DAKJDA	success or wait	1	40D2CF	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\HDGIJJ	success or wait	1	40C61C	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\HIEBAK	success or wait	1	40D0C0	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\EBGCBA	success or wait	1	406DC5	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\EBKJDB	success or wait	1	40D2CF	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\FCGCGD	success or wait	1	40C61C	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\JDGCGD	success or wait	1	40D0C0	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\KKJEBA-shm	success or wait	2	1B495612	DeleteFileW
C:\ProgramData\FCGCGDHJEGHJ\KKJEBA	success or wait	1	408CAA	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\KJKJJJ-shm	success or wait	2	1B495612	DeleteFileW
C:\ProgramData\FCGCGDHJEGHJ\KJKJJJ	success or wait	1	409480	DeleteFileA
C:\ProgramData\FCGCGDHJEGHJ\GCGDGH	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\T9RRWRNL\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"><<	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\53IVYM2Y\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.$7ZYZYZYZnY\Y] Y XYYZXYO\EYO]UYOZLY l3][Yl3Y[Yl3[Yl3[[YRichZY	success or wait	2254	40433D	InternetReadFile
C:\ProgramData\FCGCGDHJEGHJ\DHDHJJ	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	4068AE	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\DAKJDA	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 01 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 01 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 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	40D1D9	CopyFileA
C:\ProgramData\FCGCGDHJEGHJ\HDGIJJ	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\FCGCGDHJEGHJ\HIEBAK	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	SQLite format 3@ 4!.j1	success or wait	1	40CF40	CopyFileA
C:\ProgramData\FCGCGDHJEGHJ\EBGCBA	0	20480	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 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 05 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 07 00 2e 6a fd 0d 0d 24 00 04 0a 0c 00 0f 67 0f fd 0a 0c 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j$g	success or wait	1	4068AE	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\EBKJDB	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 01 00 00 00 26 00 00 00 00 00 00 00 00 00 00 00 1f 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 01 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	SQLite format 3@ &.j	success or wait	2	40D1D9	CopyFileA
C:\ProgramData\FCGCGDHJEGHJ\FCGCGD	0	51200	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 19 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 01 00 2e 6a fd 05 00 00 00 02 07 fd 00 00 00 00 18 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 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\FCGCGDHJEGHJ\JDGCGD	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 36 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 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y6.jW	success or wait	2	40CF40	CopyFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\freebl3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	621	404ECE	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\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 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 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
C:\ProgramData\FCGCGDHJEGHJ\JDGCGD	0	1024	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 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 36 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 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y6.jW	success or wait	583	404ECE	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\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 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.$PEL4c"!^j@A`W,	success or wait	594	404EAA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\freebl3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	414	404ECE	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\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 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.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	440	404EAA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\nss3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1874	404ECE	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\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 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 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 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 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.$PEL4c"!.`pl-@A&@	success or wait	1999	404EAA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\softokn3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	237	404ECE	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\softokn3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	252	404EAA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PMW3U6MX\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 fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 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	73	404ECE	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\vcruntime140.dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"	success or wait	79	404EAA	WriteFile
C:\ProgramData\FCGCGDHJEGHJ\KKJEBA	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	1	408847	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\KJKJJJ	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	SQLite format 3@ .&K.j-a>~|0{dzzz"yy3xxKwvuuGtt;sAsqpqp{oohnnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	409223	CopyFileA
C:\ProgramData\FCGCGDHJEGHJ\GCGDGH	0	9504	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	601365	success or wait	1	406206	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\DHDHJJ	0	100	success or wait	4	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\DAKJDA	0	100	success or wait	6	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\DAKJDA	0	100	success or wait	6	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\HDGIJJ	0	100	success or wait	6	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\HIEBAK	0	100	success or wait	9	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\HIEBAK	0	100	success or wait	18	1B48FE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	44137	success or wait	1	406206	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\EBGCBA	0	100	success or wait	4	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\EBKJDB	0	100	success or wait	6	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\EBKJDB	0	100	success or wait	6	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\FCGCGD	0	100	success or wait	7	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\JDGCGD	0	100	success or wait	26	1B48FE09	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGCGDHJEGHJ\KKJEBA	0	100	success or wait	4	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\KJKJJJ	0	100	success or wait	5	1B48FE09	ReadFile
C:\ProgramData\FCGCGDHJEGHJ\GCGDGH	0	9504	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: **7044**, Parent PID: **1600**

General

Target ID:	7
Start time:	12:06:58
Start date:	17/05/2024
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\FCGCGDHJEGHJ" & exit
Imagebase:	0x790000
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: **2860**, Parent PID: **7044**

General

Target ID:	8
Start time:	12:06:58
Start date:	17/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
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: **5392**, Parent PID: **7044**

General	
Target ID:	9
Start time:	12:06:58
Start date:	17/05/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 10
Imagebase:	0x1f0000
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