ID: 1443958
Sample Name: file.exe
Cookbook: default.jbs
Time: 09:08:06
Date: 19/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

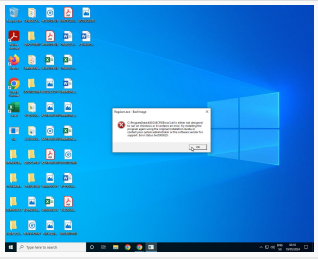
Windows Analysis Report

file.exe

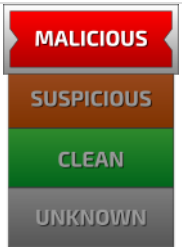
Overview

General Information

Sample name:	file.exe
Analysis ID:	1443958
MD5:	7e74918f07900..
SHA1:	0042d5e84604...
SHA256:	fed19121e9d54..
Tags:	exe
Infos:	



Detection



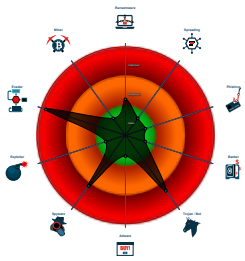
Vidar

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…
- Multi AV Scanner detection for dom…
- Yara detected AntiVM3
- Yara detected Powershell download…
- Yara detected Vidar stealer
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Contains functionality to inject code…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6708 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 7E74918F0790056546B862FA3E114C2A)
  - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - RegAsm.exe (PID: 3264 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
- **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

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.2899893197.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2899893197.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x221f0:$s1: JohnDoe • 0x221e8:$s2: HAL9TH
00000000.00000002.1645416850.0000000000158000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: file.exe PID: 6708	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:$s1: JohnDoe • 0x221e8:$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.130000.0.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
- Multi AV Scanner detection for domain / URL
- 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 stealer
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

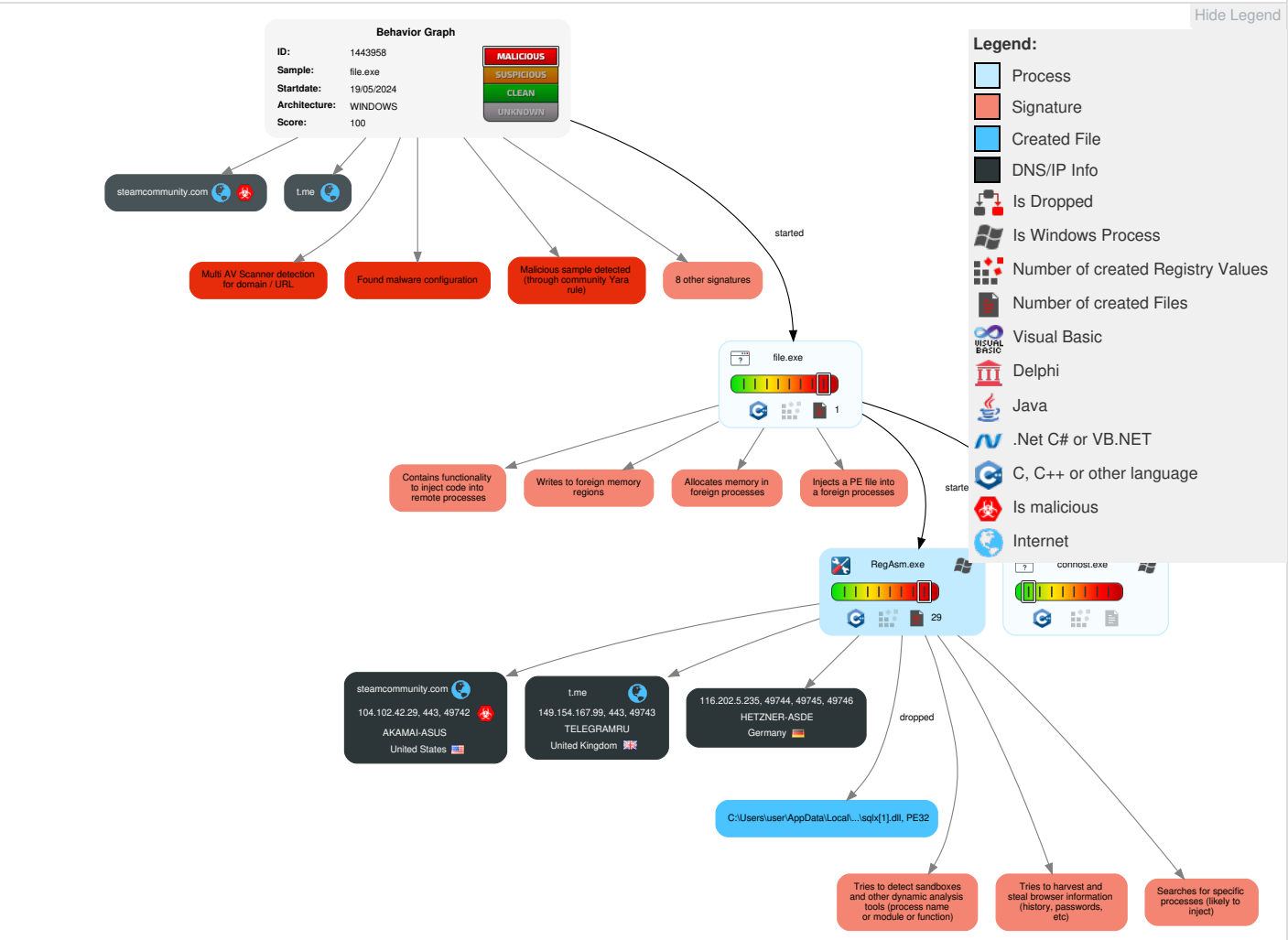
- Yara detected Vidar stealer

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	5 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Screen Capture	2 1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	5 1 1 Process Injection	LSASS Memory	1 4 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate /Decode Files or Information	Security Account Manager	1 2 Process Discovery	SMB/Windows Admin Shares	1 Data from Local System	2 Ingress Tool Transfer	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	2 Obfuscated Files or Information	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	1 3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	Steganography	Cached Domain Credentials	3 File and Directory 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	5 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery

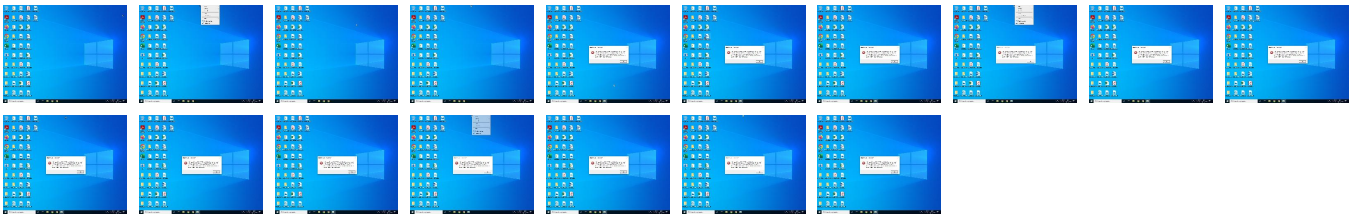
Behavior Graph



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:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
steamcommunity.com	0%	Virustotal		Browse
t.me	0%	Virustotal		Browse

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://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	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=Iy1ies1ROjUT&l=english	0%	URL Reputation	safe	
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	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://store.steampowered.com/privacy_agreement/	0%	URL Reputation	safe	
http://https://store.steampowered.com/points/shop/	0%	URL Reputation	safe	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://https://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://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=english	0%	URL Reputation	safe	
http://https://116.202.5.235:9000EB	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_logo.png	0%	URL Reputation	safe	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	0%	URL Reputation	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/?subsection=broadcasts	0%	Avira URL Cloud	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://116.202.5.235:9000/soft	100%	Avira URL Cloud	malware	
http://https://help.steampowered.com/en/	0%	URL Reputation	safe	
http://https://store.steampowered.com/news/	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://store.steampowered.com/subscriber_agreement/	0%	URL Reputation	safe	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	0%	URL Reputation	safe	
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://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://https://116.202.5.235:9000/softokn3.dllP	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
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://store.steampowered.com/	0%	URL Reputation	safe	
http://https://116.202.5.235:9000/msvcp140.dll	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw	0%	URL Reputation	safe	
http://https://116.202.5.235:9000/softokn3.dlldge	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/chrome_newtab	0%	Virustotal		Browse
http://https://steamcommunity.com/?subsection=broadcasts	0%	Virustotal		Browse
http://https://community.akamai.steamstatic.com/public/shared/images/header/logo_steam.s	0%	Virustotal		Browse
http://https://community.akamai.steamstatic.com/public/shared/images/header/logo_steam.s	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=6MtR	0%	Avira URL Cloud	safe	
http://https://116.202.5.235:9000/mozglue.dllEdge	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIlcMzCffX6&	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	0%	Avira URL Cloud	safe	
http://https://116.202.5.235:9000/nss3.dll2	100%	Avira URL Cloud	malware	
http://https://116.202.5.235:9000/softokn3.dllf	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=6MtR	0%	Virustotal		Browse
http://https://116.202.5.235:9000/freebl3.dllEdge	100%	Avira URL Cloud	malware	
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIlcMzCffX6&	0%	Virustotal		Browse
http://https://116.202.5.235:9000	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/ac/?q=	0%	Virustotal		Browse
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	0%	Virustotal		Browse
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	0%	Virustotal		Browse
http://https://116.202.5.235:9000/vcruntime140.dllets	100%	Avira URL Cloud	malware	
http://https://116.202.5.235:9000/msvcp140.dlldge	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199686524322	0%	Avira URL Cloud	safe	
http://https://116.202.5.235:9000/sqlx.dll	100%	Avira URL Cloud	malware	
http://https://116.202.5.235:9000ing	0%	Avira URL Cloud	safe	
http://https://116.202.5.235:9000	3%	Virustotal		Browse
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/_	0%	Avira URL Cloud	safe	
http://https://116.202.5.235:9000/softokn3.dll	100%	Avira URL Cloud	malware	
http://https://116.202.5.235:9000/sqlx.dll	10%	Virustotal		Browse
http://https://116.202.5.235:9000/softokn3.dll2	100%	Avira URL Cloud	malware	
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/globalv2.css?v=PAcV2zMBzzSV&l=english	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Virustotal		Browse
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199686524322	0%	Virustotal		Browse
http://https://116.202.5.235:9000/nss3.dllft	100%	Avira URL Cloud	malware	
http://https://116.202.5.235:9000/vcruntime140.dllUser	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/my/wishlist/	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english	0%	Virustotal		Browse
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	0%	Virustotal		Browse
http://https://t.me/	0%	Avira URL Cloud	safe	
http://https://web.telegram.org	0%	Avira URL Cloud	safe	
http://https://116.202.5.235:9000/vcruntime140.dll.	100%	Avira URL Cloud	malware	
http://https://t.me/	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://116.202.5.235:9000/v	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/_	0%	Virustotal		Browse
http://https://steamcommunity.com/market/	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://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	0%	Avira URL Cloud	safe	
http://https://116.202.5.235:9000/mozglue.dll	100%	Avira URL Cloud	malware	
http://https://web.telegram.org	0%	Virustotal		Browse
http://https://steamcommunity.com/market/	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
steamcommunity.com	104.102.42.29	true	true	• 0%, Virustotal, Browse	unknown
t.me	149.154.167.99	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://t.me/k0mono	false	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://116.202.5.235:9000EB	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	FHJEGI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	FHJEGI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/?subsection=broadcasts	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/soft	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/softokn3.dllP	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/msvcp140.dll	RegAsm.exe, 00000002.00000002.2900946263.0000000013E9000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2900806294.0000000001380000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/softokn3.dllIdge	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/header/logo_steam.s	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.valvesoftware.com/legal.htm	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/promo/summer2017/stickers.css?v=HA2Yr5oy3FFG&	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/mozglue.dllEdge	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.png	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIlcMzCffX6&	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/nss3.dll2	RegAsm.exe, 00000002.00000002.2900946263.00000000013E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

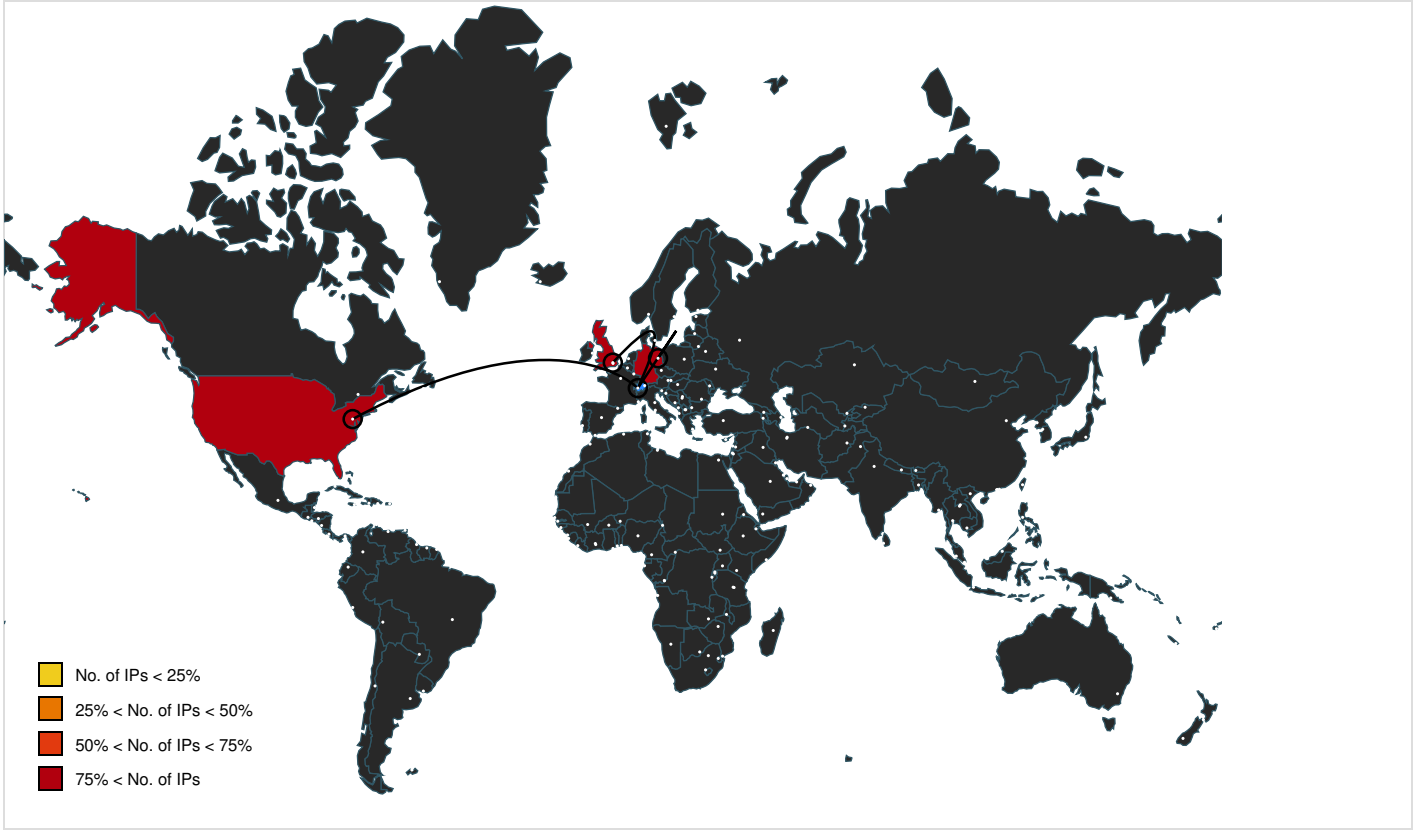
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/softokn3.dllf	RegAsm.exe, 00000002.00000002.2900946263.00000000013E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/freebl3.dllEdge	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/css/skin_1/header.css?v=NFoCa4OkAxRb&l=english	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000	RegAsm.exe, 00000002.00000002.2899893197.0000000000523000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000586000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/vcruntime140.dllets	RegAsm.exe, 00000002.00000002.2900806294.000000000138F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/msvcp140.dlldge	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199686524322	76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/sqlx.dll	RegAsm.exe, 00000002.00000002.2899893197.0000000000561000.00000040.00000400.00020000.00000000.sdmp	false	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000ing	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/points/shop/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	FHJEGI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/_	RegAsm.exe, 00000002.00000002.2900507814.0000000001272000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp, DHCFID.2.dr	false	• URL Reputation: safe	unknown
http://https://www.ecosia.org/newtab/	FHJEGI.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/softokn3.dll	RegAsm.exe, 00000002.00000002.2900946263.00000000013E9000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/softokn3.dll2	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=english	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_logo.png	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	DHCFID.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/nss3.dllft	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://store.steampowered.com/about/	76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/vcruntime140.dllUser	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/my/wishlist/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://t.me/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/vcruntime140.dll.	RegAsm.exe, 00000002.00000002.2900806294.000000000138F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://web.telegram.org	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000523000.00000040.00000400.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/v	RegAsm.exe, 00000002.00000002.2900987028.00000000013F7000.00000004.00000020.00020000.00000000.sdmp	false	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://help.steampowered.com/en/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/market/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.steampowered.com/news/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/applications/community/main.css?v=5CgcHEsWGAFt&a	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	FHJEGI.2.dr	false	• URL Reputation: safe	unknown
http://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp, DHCFID.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/mozglue.dll	RegAsm.exe, 00000002.00000002.2900946263.00000000013E9000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/	RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/f	RegAsm.exe, 00000002.00000002.2900987028.00000000013F7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/javascript/promo/stickers.js?v=upl9NJ5D2xkP&l=en	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://116.202.5.235:9000/b	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/discussions/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/vcruntime140.dllO	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://store.steampowered.com/stats/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/steam_refunds/	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	DHCFID.2.dr	false	• URL Reputation: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	FHJEGI.2.dr	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/profiles/76561199686524322/inventory/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity.com/profiles/76561199686524322/badges	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: malware	unknown
http://https://steamcommunity.com/workshop/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/legal/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000002.00000002.2901515013.00000000134DC000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2905345080.000000001947D000.00000002.00001000.00020000.00000000.sdmp, sqlx[1].dll.2.dr	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/main.js?v=soQOTmUz	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, 76561199686524322[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/vcruntime140.dllh	RegAsm.exe, 00000002.00000002.2900806294.000000000138F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v=pSv	RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	FHJEGI.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.5.235:9000/msvcp140.dllD	RegAsm.exe, 00000002.00000002.2900806294.0000000001380000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/vcruntime140.dllc	RegAsm.exe, 00000002.00000002.2900806294.000000000138F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235:9000/freebl3.dll	RegAsm.exe, 00000002.00000002.2900946263.00000000013E9000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.00000000005A5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.5.235/	RegAsm.exe, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	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, 00000002.00000002.2900666615.00000000012A5000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.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
116.202.5.235	unknown	Germany		24940	HETZNER-ASDE	false
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1443958
Start date and time:	2024-05-19 09:08:06 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 6m 4s
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:	7
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@4/9@2/3
EGA Information:	• Successful, ratio: 100%

HCA Information:	• Successful, ratio: 95% • 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): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): slscr.update.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, umwatson.events.data.microsoft.com, fe3cr.delivery.mp.microsoft.com
- 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:09:04	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\KJDGIJECFIEB\DHCFID

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UIYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0

SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\ProgramData\KJDGIJECFIEB\EBAEBF

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F798 38
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\KJDGIJECFIEB\FHJEGI

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

C:\ProgramData\KJDGIJECFIEB\GCGHJE

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A

SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4457 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\KJDGIJECFIEB\HDBGDH

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	modified
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\ProgramData\KJDGIJECFIEB\KFBAEC

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\KJDGIJECFIEB\KJDGIJ

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 11, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.5793180405395284
Encrypted:	false
SSDEEP:	96:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7Yltnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C278196210 3
Malicious:	false

Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199686524322[1].htm	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (2969), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	34714
Entropy (8bit):	5.386623198503238
Encrypted:	false
SSDEEP:	768:Ddpqm+0Ih3YAA9CWGA0fcDAZPzzgiJmDzJtxvrfJkPVoEAdmPzzgiJmDzJtxvJ2T:Dd8m+0Ih3YAA9CWGA0FZPzzgiJmDzJtM
MD5:	1EF9C3C348E57460F3B94FC645431042
SHA1:	D91B82D9167E99DDB141F71EB8EB6EF609860D0C
SHA-256:	5F76FC8FE5351E2BF0C07C3A09D0B83F82F0B7F953537E4AB0EC025BB79798D3
SHA-512:	639CC2EF6CD5B8ED8EC35D4D40EE361AEABC4D8E09F09D6F175DA5DC6AD257221C298871248228734AFF064F9CF5E3F7E2064B6813D36A65FDCC91980242D7B5
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 :: 76561199686524322</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 href="https:/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2459136
Entropy (8bit):	6.052474106868353
Encrypted:	false
SSDEEP:	49152:WHoJ9zGioiMjW2RrL9B8SSpiCH7cuez9A:WHoJBGqabRnj8JY/9
MD5:	90E744829865D57082A7F452EDC90DE5
SHA1:	833B178775F39675FA4E55EAB1032353514E1052
SHA-256:	036A57102385D7F0D7B2DEACF932C1C372AE30D924365B7A88F8A26657DD7550
SHA-512:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E570323
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..... .....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.557280266846168
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:	372'736 bytes
MD5:	7e74918f0790056546b862fa3e114c2a
SHA1:	0042d5e84604f4e144ea0795db36839c50d8ed1f
SHA256:	fed19121e9d547d9762e7aa6dd53e0756c414bd0a0650e38d6b0c01b000ad2fc

SHA512:	684cfcf2f81398156460d8bb956897b6f0b4e1e230c187028c488d782305ec978eee657d3f536c7f8c431ada37f77f6398b03abe339af9ddae1dd66a5e9d2550
SSDEEP:	6144:SjyaaHbrb0YCCx3TkA1tiyGZnoi78XUeaiRkm09DLnWyYtR8/8yDe9a6n:eyaa7L1tiF2U6aas9votR8/BEFn
TLSH:	2684D051B1C0C071E56325364AF0DBB15E3EF9704FA15ECF67A40BBE4F30691DA21AAA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r.....a.....a..k....a.....a.....2.....2.....Rich.....PE..L..

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x40527b
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:	0x66490AA4 [Sat May 18 20:08:04 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:	65f8d3b7633d5a017c9f24a26c67363d

Entrypoint Preview

Instruction
call 00007F6260DFF85Eh
jmp 00007F6260DFEF29h
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 00007F6260DFEE15h
jmp 00007F6260DFF092h
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

Instruction
mov ebp, eax
mov eax, dword ptr [0045A540h]
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 [0045A540h]
xor eax, ebp
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 [0045A540h]
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	0x26b6c	0x3c	.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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x1e000	0x164	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

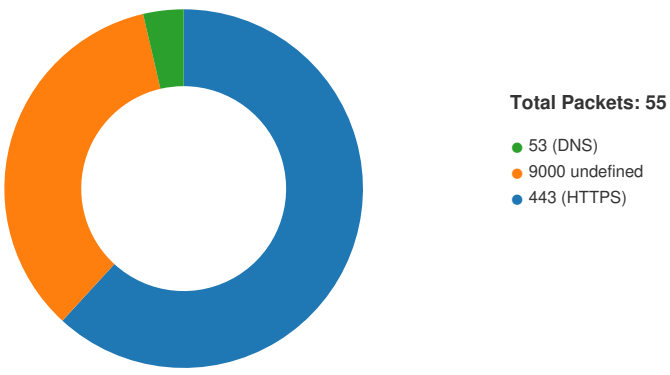
Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1bb3f	0x1bc00	896aa19da20dfcddfae4daf6f2295875	False	0.5772628096846847	data	6.600341435678309	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.bsS	0x1d000	0xa84	0xc00	3a54c614cecfd0e64b884f3c41c32ad4	False	0.5911458333333334	data	5.946566168578569	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1e000	0x9390	0x9400	05f792426862b0e0eea2c0e5e390047d	False	0.39263091216216217	data	4.707613266129105	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x28000	0x3437c	0x33400	c91ec62c4af8d334d85a9e884d07d303	False	0.9840844131097561	data	7.984093459079469	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x5d000	0x1a54	0x1c00	988e3cd821783dfbb1c13de905f594d2	False	0.7306082589285714	data	6.373828393083266	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ADVAPI32.dll	CryptDecrypt
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 19, 2024 09:08:56.125937939 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:56.126024008 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:56.126138926 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:56.133630037 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:56.133694887 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:56.851352930 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:56.851444960 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:56.899281025 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:56.899349928 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:56.900289059 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:56.900363922 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:56.904191971 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:56.948194027 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.502080917 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.502147913 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.502187967 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.502226114 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.502253056 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.502271891 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.502312899 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.502396107 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.608273983 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.608345985 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.608419895 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.608459949 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.608494043 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.608516932 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.615500927 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.615602016 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.615669012 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.615717888 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.615736961 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.615792036 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.615892887 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.615945101 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.655944109 CEST	49742	443	192.168.2.4	104.102.42.29
May 19, 2024 09:08:57.656008959 CEST	443	49742	104.102.42.29	192.168.2.4
May 19, 2024 09:08:57.727955103 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:57.727981091 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:57.728126049 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:57.730151892 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:57.730170965 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.466494083 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.466582060 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.498569965 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.498588085 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.499627113 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.499799013 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.519278049 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.564121962 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.761395931 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.761454105 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.761456966 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.761491060 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.761517048 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.761533022 CEST	443	49743	149.154.167.99	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 09:08:58.761548996 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.761559963 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.761580944 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.761607885 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.761615992 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.761647940 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.761672974 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.761718988 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.769680977 CEST	49743	443	192.168.2.4	149.154.167.99
May 19, 2024 09:08:58.769695997 CEST	443	49743	149.154.167.99	192.168.2.4
May 19, 2024 09:08:58.784607887 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:58.817583084 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:08:58.817748070 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:58.824115992 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:58.869514942 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:08:59.523859978 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:08:59.523947954 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:59.528754950 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:08:59.528809071 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:59.551728010 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:59.578005075 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:08:59.776231050 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:08:59.776339054 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:59.776804924 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:08:59.829636097 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:09:00.292948961 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:09:00.293068886 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:00.296513081 CEST	49745	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:00.345664978 CEST	9000	49745	116.202.5.235	192.168.2.4
May 19, 2024 09:09:00.345810890 CEST	49745	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:00.346107006 CEST	49745	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:00.397767067 CEST	9000	49745	116.202.5.235	192.168.2.4
May 19, 2024 09:09:01.030155897 CEST	9000	49745	116.202.5.235	192.168.2.4
May 19, 2024 09:09:01.030241013 CEST	49745	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:01.151000977 CEST	49745	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:01.156008005 CEST	9000	49745	116.202.5.235	192.168.2.4
May 19, 2024 09:09:01.156707048 CEST	49745	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:01.161905050 CEST	9000	49745	116.202.5.235	192.168.2.4
May 19, 2024 09:09:01.831651926 CEST	9000	49745	116.202.5.235	192.168.2.4
May 19, 2024 09:09:01.831751108 CEST	49745	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:01.850370884 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:01.855834961 CEST	9000	49744	116.202.5.235	192.168.2.4
May 19, 2024 09:09:01.855914116 CEST	49744	9000	192.168.2.4	116.202.5.235
May 19, 2024 09:09:01.870893002 CEST	49746	9000	192.168.2.4	116.202.5.235

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 09:08:56.110912085 CEST	62675	53	192.168.2.4	1.1.1.1
May 19, 2024 09:08:56.119693995 CEST	53	62675	1.1.1.1	192.168.2.4
May 19, 2024 09:08:57.719383955 CEST	58308	53	192.168.2.4	1.1.1.1
May 19, 2024 09:08:57.727220058 CEST	53	58308	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 19, 2024 09:08:56.110912085 CEST	192.168.2.4	1.1.1.1	0xbb2d	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false
May 19, 2024 09:08:57.719383955 CEST	192.168.2.4	1.1.1.1	0x80a9	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false

DNS Answers

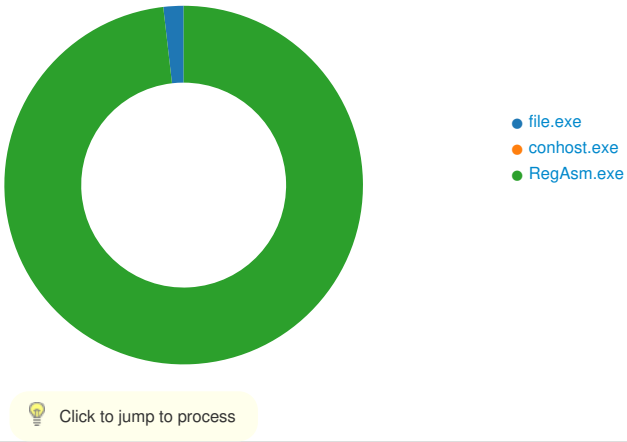
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 19, 2024 09:08:56.119693995 CEST	1.1.1.1	192.168.2.4	0xbb2d	No error (0)	steamcommunity.com		104.102.42.29	A (IP address)	IN (0x0001)	false
May 19, 2024 09:08:57.727220058 CEST	1.1.1.1	192.168.2.4	0x80a9	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com
- t.me

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **6708**, Parent PID: **2580**

General

Target ID:	0
Start time:	03:08:54
Start date:	19/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x130000
File size:	372'736 bytes
MD5 hash:	7E74918F0790056546B862FA3E114C2A
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: 00000000.00000002.1645416850.0000000000158000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: 6728, Parent PID: 6708

General

Target ID:	1
Start time:	03:08:54
Start date:	19/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 3264, Parent PID: 6708

General

Target ID:	2
Start time:	03:08:55
Start date:	19/05/2024
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:	0xad0000
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: 00000002.00000002.2899893197.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000002.00000002.2899893197.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000002.00000002.2899893197.0000000000446000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\KJDGIJECFIEB	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
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\KJDGIJECFIEB\KJDGIJ	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\KJDGIJECFIEB\DHCFID	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\KJDGIJECFIEB\KFBAEC	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\KJDGIJECFIEB\FHJEGI	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\KJDGIJECFIEB\EBAEBF	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\KJDGIJECFIEB\GCGHJE	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\KJDGIJECFIEB\HDBGDH	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\KJDGIJECFIEB\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\KJDGIJECFIEB\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\KJDGIJECFIEB\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\KJDGIJECFIEB\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\KJDGIJECFIEB\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\KJDGIJECFIEB\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\KJDGIJECFIEB\KJDGIJ	success or wait	1	406DC5	DeleteFileA
C:\ProgramData\KJDGIJECFIEB\DHCFID	success or wait	1	40D2CF	DeleteFileA
C:\ProgramData\KJDGIJECFIEB\KFBAEC	success or wait	1	40C61C	DeleteFileA
C:\ProgramData\KJDGIJECFIEB\FHJEGI	success or wait	1	40D0C0	DeleteFileA
C:\ProgramData\KJDGIJECFIEB\EBAEBF	success or wait	1	40D2CF	DeleteFileA
C:\ProgramData\KJDGIJECFIEB\GCGHJE	success or wait	1	40C61C	DeleteFileA
C:\ProgramData\KJDGIJECFIEB\HDBGDH	success or wait	1	40D0C0	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199686524322[1].htm	0	1999	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 20 72 65 73 70 6f 6e 73 69 76 65 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0d 0a 09 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 68 65 6d 65 2d 63 6f 6c 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 23 31 37 31 61 32 31 22 3e 0d 0a 09 09 3c	<!DOCTYPE html><html class=" responsive" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1"> <meta name="theme-color" content="#171a21"> <	success or wait	17	4050D8	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1e fd 37 fd 5a fd 59 fd 5a fd 59 fd 5a fd 59 fd 11 fd 5a fd 6e fd 59 fd 11 fd 5c fd f3 59 fd 11 fd 5d fd 7f fd 59 fd 11 fd 58 fd 59 fd 59 fd 5a fd 58 fd 33 59 fd 4f fd 5c fd 45 fd 59 fd 4f fd 5d fd 55 fd 59 fd 4f fd 5a fd 4c fd 59 fd 6c 33 5d fd 5b fd 59 fd 6c 33 59 fd 5b fd 59 fd 6c 33 fd fd 5b fd 59 fd 6c 33 5b fd 5b fd 59 fd 52 69 63 68 5a fd 59 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7ZYZYZYZnY\Y]Y XYYZXYO\EYO]UYOZLYl3][Yl3Y[Yl3[Yl3[[YRichZY	success or wait	2257	40433D	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\KJDGIJECFIEB\KJDGIJ	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0b 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
C:\ProgramData\KJDGIJECFIEB\DHCFID	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	40D1D9	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\KJDGIJECFIEB\KFBAEC	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 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 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	40C37E	CopyFileA
C:\ProgramData\KJDGIJECFIEB\FHJEGI	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 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\KJDGIJECFIEB\EBAEBF	0	126976	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40D1D9	CopyFileA
C:\ProgramData\KJDGIJECFIEB\GCGHJE	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40C37E	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\KJDGIJECFIEB\HDBGDH	0	114688	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 38 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 8$.O}4	success or wait	1	40CF40	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	66646	success or wait	1	406206	ReadFile
C:\ProgramData\KJDGIJECFIEB\KJDGIJ	0	100	success or wait	6	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\DHCFID	0	100	success or wait	12	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\KFBAEC	0	100	success or wait	6	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\FHJEGI	0	100	success or wait	9	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\FHJEGI	0	100	success or wait	18	1923FE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	406206	ReadFile
C:\ProgramData\KJDGIJECFIEB\EBAEBF	0	100	success or wait	6	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\EBAEBF	0	100	success or wait	6	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\GCGHJE	0	100	success or wait	6	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\HDBGDH	0	100	success or wait	10	1923FE09	ReadFile
C:\ProgramData\KJDGIJECFIEB\HDBGDH	0	100	success or wait	10	1923FE09	ReadFile

Disassembly

No disassembly