ID: 1435613
Sample Name: file.exe
Cookbook: default.jbs
Time: 23:45:04
Date: 02/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

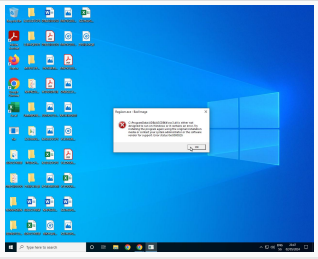
Windows Analysis Report

file.exe

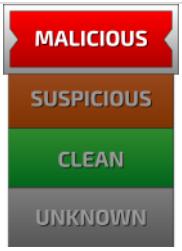
Overview

General Information

Sample name:	file.exe
Analysis ID:	1435613
MD5:	1a6b4d357d1b…
SHA1:	70961ace92a0…
SHA256:	09ad84f8dde51..
Tags:	exe
Infos:	



Detection



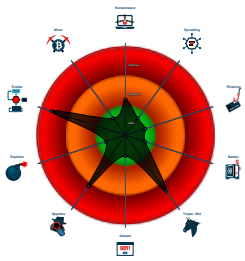
Vidar

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected Vidar stealer
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Found evasive API chain (may stop…
- Injects a PE file into a foreign proce…
- Machine Learning detection for sam…
- Searches for specific processes (lik…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6608 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 1A6B4D357D1B8BAB80524E40BE1B2698)
  - conhost.exe (PID: 6568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - RegAsm.exe (PID: 416 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/76561199680449169"
  ],
  "Botnet": "03cea2609023d13f145ac6c5dc897112",
  "Version": "9.3"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.2862223964.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.2862223964.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x201f8:$s1: JohnDoe • 0x2ef80:$s1: JohnDoe • 0x201f0:$s2: HAL9TH
00000000.00000002.1607514385.0000000000E1D000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: file.exe PID: 6608	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 416	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.e1f040.1.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.file.exe.e1f040.1.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x1e7f8:$s1: JohnDoe • 0x1e7f0:$s2: HAL9TH
0.2.file.exe.e1f040.1.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.file.exe.e1f040.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x1f3f8:$s1: JohnDoe • 0x1f3f0:$s2: HAL9TH
2.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 5 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

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

Found evasive API chain (may stop execution after checking computer name)

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

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

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

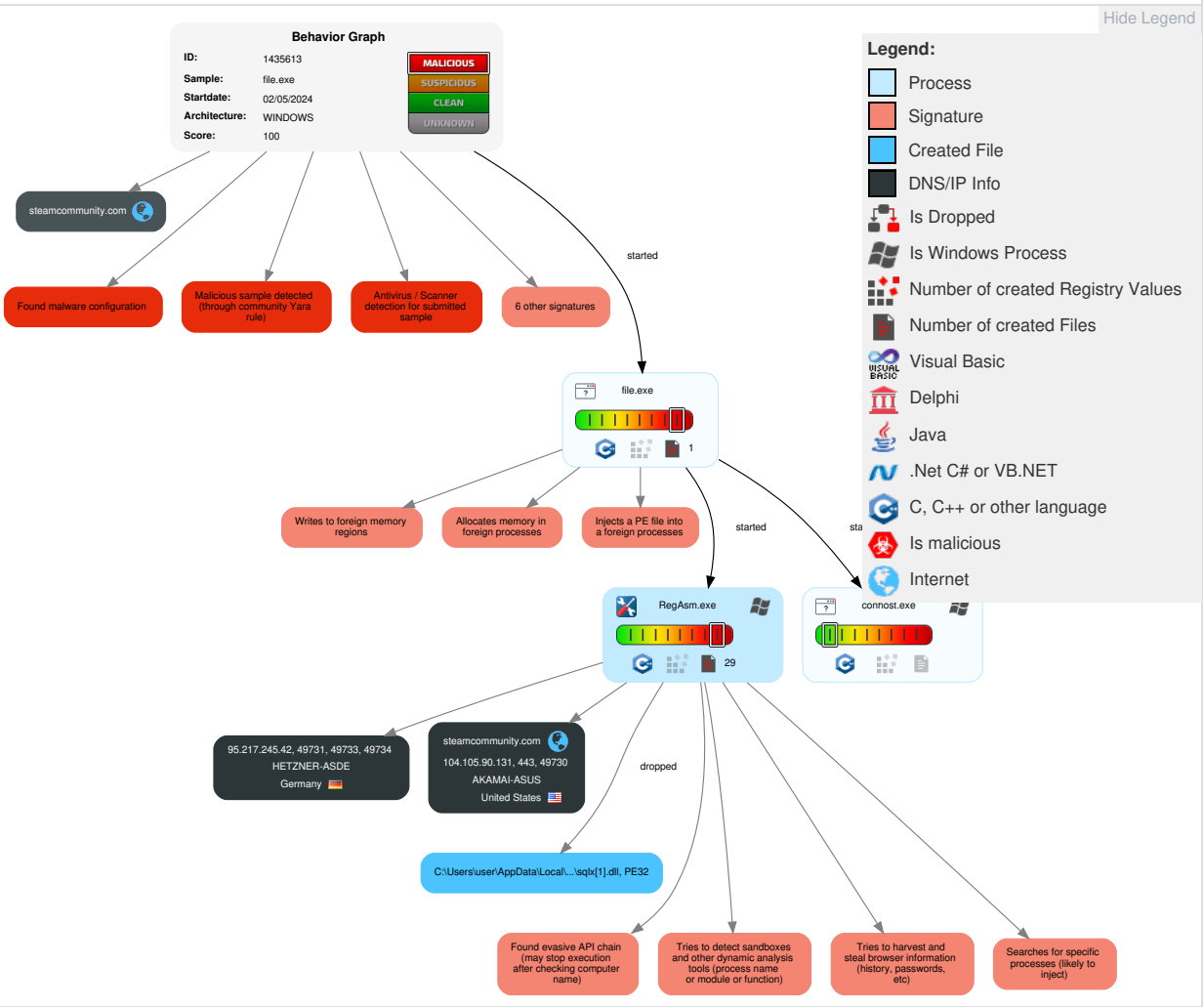
Yara detected Vidar stealer

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	4 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 1 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	4 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 Software Packing	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	1 DLL Side-Loading	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	1 5 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery

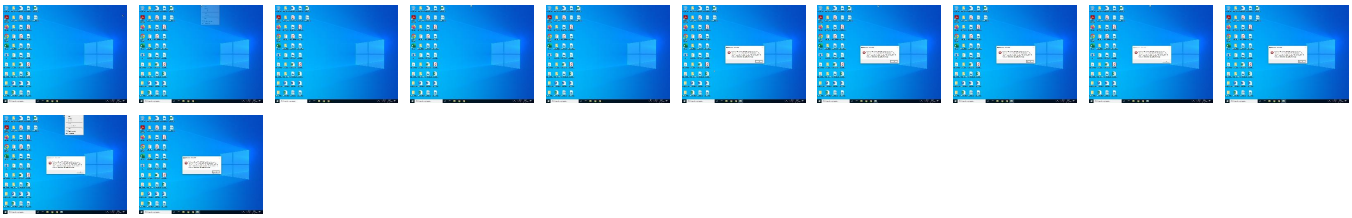
Behavior Graph



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	39%	ReversingLabs	Win32.Trojan.Generic	
file.exe	100%	Avira	HEUR/AGEN.1317595	
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

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://recaptcha.net	0%	URL Reputation	safe	
http://https://www.gstatic.cn/recaptcha/	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/r	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/mozglue.dll	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/z	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/msvcp140.dlldge	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/nss3.dll)))	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000l	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/nss3.dllD	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/nss3.dllft	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:900090ea2le	0%	Avira URL Cloud	safe	
http://https://95.217.245.42/	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/softokn3.dll	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/mozglue.dllt	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000vcruntime140.dllUser	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/mozglue.dllEdge	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/softokn3.dlldge	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/0ea2osoft	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000acrosoft	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/vcruntime140.dllser	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/nss3.dll	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/freebl3.dllEdge	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000el	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/vcruntime140.dllw=	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/msvcp140.dll	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/J	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/vcruntime140.dll_7)	0%	Avira URL Cloud	safe	
http://https://95.217.245.42:9000/B	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
steamcommunity.com	104.105.90.131	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity.com/profiles/76561199680449169	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	BKKFHIEG.2.dr	false		high
http://https://duckduckgo.com/ac/?q=	BKKFHIEG.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=_Vry	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://steamcommunity.com/?subsection=broadcasts	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/mozglue.dll	RegAsm.exe, 00000002.00000002.2862223964.0000000000528000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000/r	RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://www.gstatic.cn/recaptcha/	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/libraries~b28b7af6	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/modalContent.js?v=L35TrLJDfqtD&l=engl	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/z	RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000/msvcp140.dlldge	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000	76561199680449169[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.valvesoftware.com/legal.htm	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/promo/summer2017/stickers.css?v=HA2Yr5oy3FFG&	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.png	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIIcMzCffX6&	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/profile.js?v=Iy1ies1ROjUT&l=english	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000l	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://95.217.245.42:9000/nss3.dllD	RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000/nss3.dll)))	RegAsm.exe, 00000002.00000002.2862938128.000000000156D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/Z	RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://https://95.217.245.42:9000/nss3.dllft	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42/	RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:900090ea2le	RegAsm.exe, 00000002.00000002.2862223964.000000000056C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://community.akamai.steamstatic.com/public/css/skin_1/header.css?v=NFoCa4OkAxRb&l=english	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/softokn3.dll	RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/points/shop/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	BKKFHIEG.2.dr	false		high

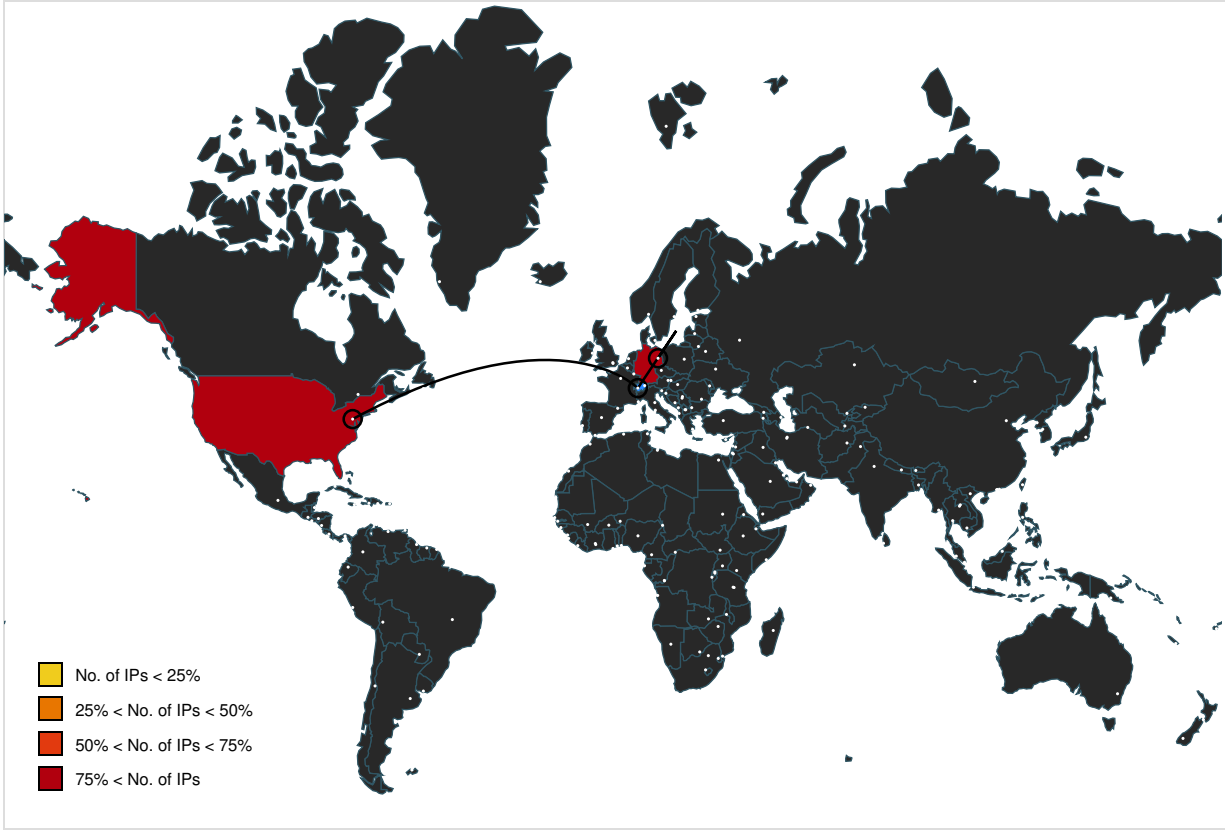
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp, CGDGCFBA.2.dr	false		high
http://https://steamcommunity.com/profiles/76561199680449169/badges	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://www.ecosia.org/newtab/	BKKFHIEG.2.dr	false		high
http://https://www.youtube.com/	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://avatars.akamai.steamstatic.com/fef49e7fa7e1997310d705b2a6158ff8dc1cdfeb_full.jpg	76561199680449169[1].htm.2.dr	false		high
http://https://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://steamcommunity.com/X	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://95.217.245.42:9000vcruntime140.dllUser	RegAsm.exe, 00000002.00000002.2862223964.000000000056C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://community.akamai.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000/mozglue.dllt	RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_global.js?v=REEGJU1hwkYI&am	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://www.google.com/recaptcha/	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://95.217.245.42:9000/mozglue.dllEdge	RegAsm.exe, 00000002.00000002.2862223964.0000000000528000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=english	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/softokn3.dlldge	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_logo.png	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	CGDGCFBA.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.valvesoftware.com/en/contact?contact-person=T	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/0ea2osoft	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/about/	76561199680449169[1].htm.2.dr	false		high
http://https://steamcommunity.com/my/wishlist/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000acrosoft	RegAsm.exe, 00000002.00000002.2862223964.0000000000606000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://95.217.245.42:9000/vcruntime140.dllser	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://help.steampowered.com/en/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://cdn.akamai.steamstatic.com/steamcommunity/public/assets/	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://steamcommunity.com/market/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://store.steampowered.com/news/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/main.js?v=roSu8uqw	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/nss3.dll	RegAsm.exe, 00000002.00000002.2862938128.000000000156D000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000/freebl3.dllEdge	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000el	RegAsm.exe, 00000002.00000002.2862223964.000000000056C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	BKKFHIEG.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199680449169	76561199680449169[1].htm.2.dr	false		high
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp, CGDGCFBA.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/promo/stickers.js?v=upl9NJ5D2xkP&l=en	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://95.217.245.42:9000/vcruntime140.dllw=	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/discussions/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://t.me/r1g1o	file.exe, file.exe, 00000000.00000002.1607514385.000000000E1D000.00000004.00000001.01000000.00000003.sdmp, RegAsm.exe, RegAsm.exe, 00000002.00000002.2862223964.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://store.steampowered.com/stats/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://store.steampowered.com/steam_refunds/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	CGDGCFBA.2.dr	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	BKKFHIEG.2.dr	false		high
http://https://95.217.245.42:9000/msvcp140.dll	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://95.217.245.42:9000/vcruntime140.dll_7)	RegAsm.exe, 00000002.00000002.2862223964.000000000052E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/workshop/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.steampowered.com/legal/	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&l=e	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000002.00000002.2863327466.000000001632F000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2866748482.000000001C2DD000.00000002.00001000.00020000.00000000.sdmp, sqlx[1].dll.2.dr	false		high
http://https://95.217.245.42:9000/B	RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/applications/community/main.css?v=tlrWyaxi8ABA&a	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v=pSv	RegAsm.exe, 00000002.00000002.2862223964.0000000000435000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.2862775596.00000000013CD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.2.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=engl	76561199680449169[1].htm.2.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	BKKFHIEG.2.dr	false		high
http://https://95.217.245.42:9000/J	RegAsm.exe, 00000002.00000002.2862953478.0000000001584000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://recaptcha.net	RegAsm.exe, 00000002.00000002.2862662158.0000000001374000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1435613
Start date and time:	2024-05-02 23:45:04 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 30s
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@4/10@1/2
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 92% • 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): 72.21.81.240
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com.delivery.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-b-net.trafficmanager.net, wu.azureedge.net, 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.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
23:45:56	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\BGDAAKJJ

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\BKKFHIEG

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\BKKFHIEGDHJKECAAKKEBAFIJKF

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:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621(3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\ProgramData\CGDGCFBA

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+UlYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+Ul3iN0RSV0k3qLyj9v
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\CGHCGIID

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\GIJECGDGCBKECAKFBGCA

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A
SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4457 4
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 69993 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	69993
Entropy (8bit):	**7.99584879649948**
Encrypted:	**true**
SSDEEP:	1536:iMveRG6BWC7T2g1wGUa5QUoaIB9ttiFJG+AOQOXI0Usvwr:feRG6BX6gUaHo9tkBHiUewr
MD5:	29F65BA8E88C063813CC50A4EA544E93
SHA1:	05A7040D5C127E68C25D81CC51271FFB8BEF3568
SHA-256:	1ED81FA8DFB6999A9FEDC6E779138FFD99568992E22D300ACD181A6D2C8DE184
SHA-512:	E29B2E92C496245BED3372578074407E8EF8882906CE10C35B3C8DEEBFEFE01B5FD7F3030ACAA693E175F4B7ACA6CD7D8D10AE1C731B09C5FA19035E005DE3 AA
Malicious:	false
Preview:	MSCF....i.....,.....I.....oXAy .authroot.stl.Ez..Q6..CK..<Tk...p.k..1...3...[..%Y.f..."K.6)..[*I.hOB."..rK.RQ*..}f..f...}....9.|.....gA...30.,O2L...0..%.U...U.t.....`dqM2.x ..t...<(uad.c...x5V.x..t..agd.v.....i...KD..q(. ...JJ.....#..'=. ...3.x...}...+T.K..!.'.`w .!.x.r.....YafhG..O.3....'P[..'.D../....n..t....R<..=\E7L0?{..T.f...ID...,...r....3z..O/.b.lwx.. .o...a\. s.....".'.....<;s.[...l...6.)ll..B.P.....k.... k0.".t!/,.....{...P8....B..0(.. .Q.....d...q,\.$.n.Q.\.p...R..:.hr./..8.S<a.s...+#3....D..h1.a.0....{.9.....:e.....n.~G.{.M.1..OU.....B.Q..y_>.P{...}i .=.a..QQT.U..\|!.pyCD@.....l..70..w..)...W^.`l...%Y.\.....i..=hYV.O8W@P.=.r.=..1m..1....)\.p..\|.c.3..t..[...).....l.{.Y....\S.....y....[.mCt....Js;...H....Q..F.....g.O...[..A.=...F[..z....k. ..mo.lW{`....O...T.g.Y.Uh.;m.'.N..f..}4..9i..t4p_bl..`.....Ie..l.P.... ...Lg.....[....5g...~D.s.h'>n.m.c.7...-..P.gG...i$...v.m.b[.yO.P/*.YH.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.139206469813435
Encrypted:	false
SSDEEP:	6:kKNE/lDN+SkQlPlEGYRMY9z+4KlDA3RUeVlWl/Vt:FSlMkPlE99SNxAhUeVLVt
MD5:	277583C13263F9525C5E77A13724E844
SHA1:	D008CCD731B24CC241A47C8822E3F8080BADBF45
SHA-256:	732D15B2D0D05C5DEBB686ACD7E3FEC42EA2BEC7324810A0F193D58D58294971
SHA-512:	A4BC61FB46CCCFD78C578E920E280D99AAA4A8115B68FD988ADD081DA1878ED963A81B4C4D60BFC8E405F62D6EDDC1F3CBBEF5B8EAEA62EBB476D6B72927CDCD
Malicious:	false
Preview:	p..... .....B....(..... .....M.....(.....i...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".b.3.6.8.5.3.8.5.a.4.7.f.d.a.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199680449169[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):	34791
Entropy (8bit):	5.384005815680116
Encrypted:	false
SSDEEP:	768:Xdpqm+0Ih3YAA9CWGEqfcDAGPzzgiJmDzJtxvrfJkPVoEAdmPzzgiJmDzJtxvJ2D:Xd8m+0Ih3YAA9CWGEqFGPzzgiJmDzJtE
MD5:	6C8C25D8CF07A6F37F1F9BEEA527C9B5
SHA1:	66719A470CC1A8D6CB4006EBD7529CDD45B9B88B
SHA-256:	63172A35E2CFC48D0E6AC7D77FAB89A36A0B68C8291F5F12F8C1F51ACFA2EF90
SHA-512:	19E91008561919E873F2BA7744D88EEC2B03B8C8B5548161A243740C8B8D1568EFB3E2647B4453D8DAF086E9D7CBD7362B8F449ED0D9690E36CF53E49D1C163
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 :: p__o https://95.217.245.42:9000|</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" >.<lin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2459136
Entropy (8bit):	6.052474106868353
Encrypted:	false
SSDEEP:	49152:WHoJ9zGioiMjW2RrL9B8SSpiCH7cuez9A:WHoJBGqabRnj8JY/9
MD5:	90E744829865D57082A7F452EDC90DE5
SHA1:	833B178775F39675FA4E55EAB1032353514E1052
SHA-256:	036A57102385D7F0D7B2DEACF932C1C372AE30D924365B7A88F8A26657DD7550
SHA-512:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E57032
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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):	7.512784715951123
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:	386'560 bytes
MD5:	1a6b4d357d1b8bab80524e40be1b2698
SHA1:	70961ace92a0ebfdb38ae27a22181fb5a4f7d440
SHA256:	09ad84f8dde519aa02e92ffce896f55271105ceaab7e0f0a1f1ca9fee90650ff
SHA512:	67484dcb04fc15b09b88679fd3ac860991cebe97c07a27bf9e425e8277def7f61d244690ee582c2be72d0dda3fa486b53382f3e3ad368602d176c5f72a77de67
SSDEEP:	6144:NqW5NIK5m09C0h5t4mnNpZO+Ua2PsQxDnK6gDeIK88JqeGq0DLt+7SHo:8W5NIYF4mnZO+Ua2zxDnKrZJqtHLt+mI
TLSH:	1684E05571C1C072D57319360AF5E6B8AE7DB8700A629EEF67980F7E0F30282D2356A7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.+z?.E)?.E)?.E)..F(3.E)..@(..E)..A(*.E)..A(-.E)..F(+.E)..D(:.E)?.D)e.E)..@(r.E)..@(>.E)...)>.E)..G(>.E)Rich?.E).....PE..L..

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x406239
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:	0x6634033C [Thu May 2 21:18:52 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:	ab27116ad46b656bb5d70aa3050a97a2

Entrypoint Preview

Instruction
call 00007FF5BC8C82A6h
jmp 00007FF5BC8C7A29h
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]

Instruction
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007FF5BC8C7BCBh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007FF5BC8C7BBCh
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007FF5BC8C7BBEh
add edx, 28h
cmp edx, esi
jne 00007FF5BC8C7B9Ch
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007FF5BC8C7BABh
push esi
call 00007FF5BC8C857Dh
test eax, eax
je 00007FF5BC8C7BD2h
mov eax, dword ptr fs:[00000018h]
mov esi, 0042E254h
mov edx, dword ptr [eax+04h]
jmp 00007FF5BC8C7BB6h
cmp edx, eax
je 00007FF5BC8C7BC2h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007FF5BC8C7BA2h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+08h], 00000000h
jne 00007FF5BC8C7BB9h
mov byte ptr [0042E258h], 00000001h
call 00007FF5BC8C7DB3h
call 00007FF5BC8CAB10h
test al, al
jne 00007FF5BC8C7BB6h
xor al, al
pop ebp
ret
call 00007FF5BC8D37B0h
test al, al
jne 00007FF5BC8C7BBCh
push 00000000h
call 00007FF5BC8CAB17h
pop ecx

Instruction
jmp 00007FF5BC8C7B9Bh
mov al, 01h
pop ebp
ret
push ebp
mov ebp, esp
cmp byte ptr [0042E259h], 00000000h
je 00007FF5BC8C7BB6h
mov al, 01h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2c5fc	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x60000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x61000	0x1a60	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2aba8	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	0x2aae8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x23000	0x140	.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	0x2120f	0x21400	0259f14c144706b277635ed1ab0291c1	False	0.5809592340225563	data	6.627111363402685	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x23000	0x9d30	0x9e00	4ac3dfb1efdf79208f4c0db2bef44157	False	0.4347804588607595	data	4.959230681067143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2d000	0x1d54	0x1000	96f6fc94400f9b3c80d126cafa6f2df3	False	0.190673828125	data	3.018020491461944	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.Left	0x2f000	0x300ec	0x30200	b0ab413fbd3df6b5d08a9255fbc8df24	False	0.9971438717532467	PGP Secret Sub-key -	7.998283255850867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x60000	0x1e0	0x200	b0719d9fb6f6593878cf5c523f13af07	False	0.52734375	data	4.701503258251789	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x61000	0x1a60	0x1c00	ffa018fa0ff6a602e133d892d6803856	False	0.7205636160714286	data	6.362035067940247	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_MANIFEST	0x60060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.5931758530183727

Imports

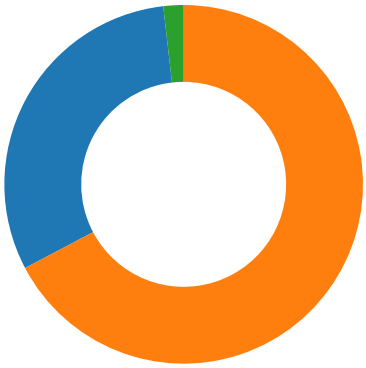
DLL	Import
USER32.dll	OpenIcon
KERNEL32.dll	LoadLibraryExW, CreateFileW, VirtualProtect, FreeConsole, WideCharToMultiByte, MultiByteToWideChar, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, EncodePointer, DecodePointer, LCMapStringEx,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

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 9000 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 2, 2024 23:45:49.704299927 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:49.704349041 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:49.704413891 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:49.710519075 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:49.710541964 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:49.898083925 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:49.898293018 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:49.945122004 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:49.945137024 CEST	443	49730	104.105.90.131	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 2, 2024 23:45:49.945533037 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:49.945590019 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:49.949198008 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:49.992119074 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.249252081 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.249279022 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.249293089 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.249346972 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.249371052 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.249394894 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.249424934 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.335556984 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.335602045 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.335634947 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.335644007 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.335675001 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.335688114 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.351237059 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.351273060 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.351311922 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:50.351313114 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.351346970 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.351368904 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.351957083 CEST	49730	443	192.168.2.4	104.105.90.131
May 2, 2024 23:45:50.351970911 CEST	443	49730	104.105.90.131	192.168.2.4
May 2, 2024 23:45:51.790647030 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:51.976289034 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:51.976366043 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:51.977089882 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:52.163177013 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:52.190546036 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:52.190625906 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:52.190629959 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:52.190674067 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:52.921133041 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.106533051 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:53.106658936 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.107150078 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.331017971 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:53.615655899 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:53.615739107 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.618604898 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.802699089 CEST	9000	49733	95.217.245.42	192.168.2.4
May 2, 2024 23:45:53.802788973 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.803042889 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.988917112 CEST	9000	49733	95.217.245.42	192.168.2.4
May 2, 2024 23:45:53.989061117 CEST	9000	49733	95.217.245.42	192.168.2.4
May 2, 2024 23:45:53.989150047 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.989566088 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:53.991019964 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.174280882 CEST	9000	49733	95.217.245.42	192.168.2.4
May 2, 2024 23:45:54.564471960 CEST	9000	49733	95.217.245.42	192.168.2.4
May 2, 2024 23:45:54.564537048 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.565793991 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.566137075 CEST	49734	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.749483109 CEST	9000	49731	95.217.245.42	192.168.2.4
May 2, 2024 23:45:54.749510050 CEST	9000	49734	95.217.245.42	192.168.2.4
May 2, 2024 23:45:54.749568939 CEST	49731	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.749615908 CEST	49734	9000	192.168.2.4	95.217.245.42

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 2, 2024 23:45:54.749953032 CEST	49734	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.934305906 CEST	9000	49734	95.217.245.42	192.168.2.4
May 2, 2024 23:45:54.934443951 CEST	9000	49734	95.217.245.42	192.168.2.4
May 2, 2024 23:45:54.934499025 CEST	49734	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.934794903 CEST	49734	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:54.936314106 CEST	49734	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:55.119627953 CEST	9000	49734	95.217.245.42	192.168.2.4
May 2, 2024 23:45:55.504204988 CEST	9000	49734	95.217.245.42	192.168.2.4
May 2, 2024 23:45:55.504230022 CEST	9000	49734	95.217.245.42	192.168.2.4
May 2, 2024 23:45:55.504267931 CEST	49734	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:55.504306078 CEST	49734	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.371469975 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.372379065 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.554893017 CEST	9000	49733	95.217.245.42	192.168.2.4
May 2, 2024 23:45:56.555012941 CEST	49733	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.555460930 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:56.555520058 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.556166887 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.744177103 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:56.744196892 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:56.744282007 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.744632006 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.746522903 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:56.929640055 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:57.303774118 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:57.303793907 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:57.303855896 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:57.303872108 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:57.303911924 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:57.303925991 CEST	9000	49735	95.217.245.42	192.168.2.4
May 2, 2024 23:45:57.303962946 CEST	49735	9000	192.168.2.4	95.217.245.42
May 2, 2024 23:45:57.303975105 CEST	9000	49735	95.217.245.42	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 2, 2024 23:45:49.608931065 CEST	58437	53	192.168.2.4	1.1.1.1
May 2, 2024 23:45:49.699968100 CEST	53	58437	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 2, 2024 23:45:49.608931065 CEST	192.168.2.4	1.1.1.1	0xe974	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false

DNS Answers

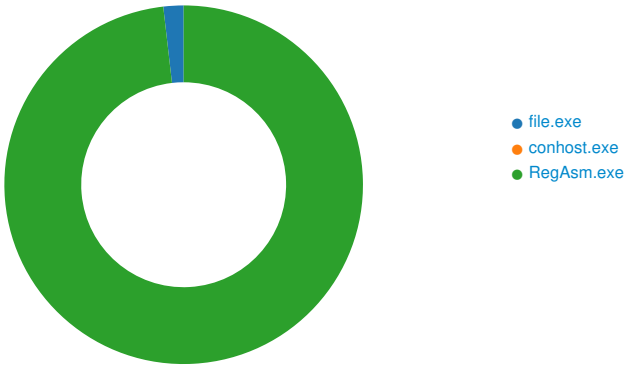
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 2, 2024 23:45:49.699968100 CEST	1.1.1.1	192.168.2.4	0xe974	No error (0)	steamcommunity.com		104.105.90.131	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: file.exe PID: 6608, Parent PID: 2580

General

Target ID:	0
Start time:	23:45:47
Start date:	02/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0xdf0000
File size:	386'560 bytes
MD5 hash:	1A6B4D357D1B8BAB80524E40BE1B2698
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: 00000000.00000002.1607514385.0000000000E1D000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: 6568, Parent PID: 6608

General

Target ID:	1
Start time:	23:45:47
Start date:	02/05/2024
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: **416**, Parent PID: **6608**

General

Target ID:	2
Start time:	23:45:48
Start date:	02/05/2024
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:	0xc60000
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: 00000002.00000002.2862223964.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000002.00000002.2862223964.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	high
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	404FFC	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	404FFC	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	404FFC	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	404FFC	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	404FFC	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	404FFC	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	404FFC	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	404FFC	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	404FFC	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	404FFC	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	404FFC	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	404FFC	HttpSendRequestA
C:\ProgramData\BKKFHIEGDHJKECAAKKEBAFIJKF	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	406830	CopyFileA
C:\ProgramData\CGDGCFBA	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	40C83E	CopyFileA
C:\ProgramData\GIJECGDGCBKECAKFBGCA	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	40BAB3	CopyFileA
C:\ProgramData\BKKFHIEG	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	40C5E8	CopyFileA
C:\ProgramData\BGDAAKJJ	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	40C83E	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\GIJECGDGCBKECAKFBGCA	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	40BAB3	CopyFileA
C:\ProgramData\CGHCGIID	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	40C5E8	CopyFileA
C:\ProgramData\JJDBAAEGDBKK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	410FD6	CreateDirectoryA
C:\ProgramData\JJDBAAEGDBKK\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E4B	CreateFileA
C:\ProgramData\JJDBAAEGDBKK\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E4B	CreateFileA
C:\ProgramData\JJDBAAEGDBKK\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E4B	CreateFileA
C:\ProgramData\JJDBAAEGDBKK\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E4B	CreateFileA
C:\ProgramData\JJDBAAEGDBKK\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E4B	CreateFileA
C:\ProgramData\JJDBAAEGDBKK\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E4B	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\BKKFHIEGDHJKECAAKKEBAFIJKF	success or wait	1	406D47	DeleteFileA
C:\ProgramData\CGDGCFBA	success or wait	1	40C934	DeleteFileA
C:\ProgramData\GIJECGDGCBKECAKFBGCA	success or wait	1	40BD53	DeleteFileA
C:\ProgramData\BKKFHIEG	success or wait	1	40C768	DeleteFileA
C:\ProgramData\BGDAAKJJ	success or wait	1	40C934	DeleteFileA
C:\ProgramData\GIJECGDGCBKECAKFBGCA	success or wait	1	40BD53	DeleteFileA
C:\ProgramData\CGHCGIID	success or wait	1	40C768	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199680449169[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	4050A0	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	2323	4042F0	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BKKFHIEGDHJKECAAKKEBAFIJKF	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0b 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	406830	CopyFileA
C:\ProgramData\CGDGCFBA	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	40C83E	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\GIJECGDGCBKECAKFBGCA	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 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 00 00 00 00 01 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40BAB3	CopyFileA
C:\ProgramData\BKKFHIEG	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	SQLite format 3@ 4!.j1	success or wait	1	40C5E8	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\BGDAAKJJ	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 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40C83E	CopyFileA
C:\ProgramData\GIJECGDGCBKECAKFBGCA	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 00 00 00 00 01 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40BAB3	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\CGHCGIID	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 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	SQLite format 3@ 8$.O}4	success or wait	1	40C5E8	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	4061B3	ReadFile
C:\ProgramData\BKKFHIEGDHJKECAAKKEBAFIJKF	0	100	success or wait	6	1C09FE09	ReadFile
C:\ProgramData\CGDGCFBA	0	100	success or wait	6	1C09FE09	ReadFile
C:\ProgramData\CGDGCFBA	0	100	success or wait	6	1C09FE09	ReadFile
C:\ProgramData\GIJECGDGCBKECAKFBGCA	0	100	success or wait	6	1C09FE09	ReadFile
C:\ProgramData\BKKFHIEG	0	100	success or wait	9	1C09FE09	ReadFile
C:\ProgramData\BKKFHIEG	0	100	success or wait	9	1C09FE09	ReadFile
C:\ProgramData\BKKFHIEG	0	100	success or wait	21	1C09FE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	4061B3	ReadFile
C:\ProgramData\GIJECGDGCBKECAKFBGCA	0	100	success or wait	6	1C09FE09	ReadFile
C:\ProgramData\CGHCGIID	0	100	success or wait	10	1C09FE09	ReadFile
C:\ProgramData\CGHCGIID	0	100	success or wait	10	1C09FE09	ReadFile

Disassembly

No disassembly