ID: 1437185
Sample Name: file.exe
Cookbook: default.jbs
Time: 05:28:06
Date: 07/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: Vidar 4
Yara Signatures 5
Initial Sample 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 6
Data Obfuscation 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 11
World Map of Contacted IPs 16
Public IPs 17
General Information 17
Warnings 17
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 18
Domains 18
ASNs 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
C:\ProgramData\AEGIJKEHCAKF\BKKFHI 18
C:\ProgramData\AEGIJKEHCAKF\GDBAKK 18
C:\ProgramData\AEGIJKEHCAKF\GHJJDG 19
C:\ProgramData\AEGIJKEHCAKF\GHJKEH 19
C:\ProgramData\AEGIJKEHCAKF\HDBKJE 19
C:\ProgramData\AEGIJKEHCAKF\IEHJJE 20
C:\ProgramData\AEGIJKEHCAKF\KFIJEG 20
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 20
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 21
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log 21
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199680449169[1].htm 21
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll 21
Static File Info 22
General 22
File Icon 22
Static PE Info 22
General 22
Authenticode Signature 23

Entrypoint Preview 23
Data Directories 24
Sections 25
Resources 25
Imports 25
Network Behavior 25
Network Port Distribution 25
TCP Packets 26
UDP Packets 27
DNS Queries 27
DNS Answers 27
HTTP Request Dependency Graph 28
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: file.exePID: 3228, Parent PID: 2580 28
General 28
File Activities 29
File Created 29
File Written 29
File Read 29
Analysis Process: RegAsm.exePID: 5816, Parent PID: 3228 29
General 29
File Activities 29
File Created 29
File Deleted 31
File Written 31
File Read 36
Disassembly 36

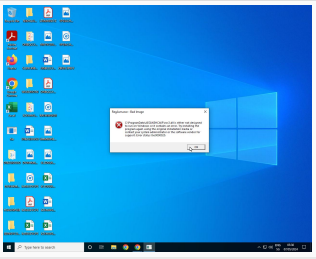
Windows Analysis Report

file.exe

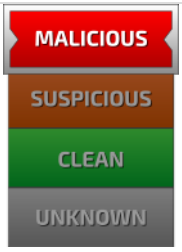
Overview

General Information

Sample name:	file.exe
Analysis ID:	1437185
MD5:	b9773393891d…
SHA1:	784a14954c7a…
SHA256:	0a8357cb9a1d…
Tags:	exe
Infos:	



Detection



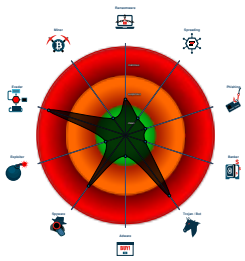
PureLog Stealer, Vidar

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected PureLog Stealer
- Yara detected Vidar stealer
- .NET source code contains method …
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Contains functionality to inject code…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 3228 cmdline: "C:\Users\user\Desktop\file.exe" MD5: B9773393891D9CC471CD58CAC09052DD)
  - RegAsm.exe (PID: 5816 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": "ad7dbf02afc50b46afd33ddc12f41082",
  "Version": "9.4"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
file.exe	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1632108400.0000000003D65000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.1628578580.00000000009A2000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
00000001.00000002.2880201060.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000001.00000002.2880201060.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x211f0:$s1: JohnDoe • 0x31f80:$s1: JohnDoe • 0x211e8:$s2: HAL9TH
Process Memory Space: file.exe PID: 3228	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 3 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.file.exe.9a0000.0.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
1.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.RegAsm.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x211f0:$s1: JohnDoe • 0x31f80:$s1: JohnDoe • 0x211e8:$s2: HAL9TH
0.2.file.exe.3d65570.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.file.exe.3d65570.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x1fbf0:$s1: JohnDoe • 0x1fbe8:$s2: HAL9TH

Click to see the 4 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for domain / URL

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)

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Searches for specific processes (likely to inject)

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected PureLog Stealer

Yara detected Vidar stealer

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

Remote Access Functionality

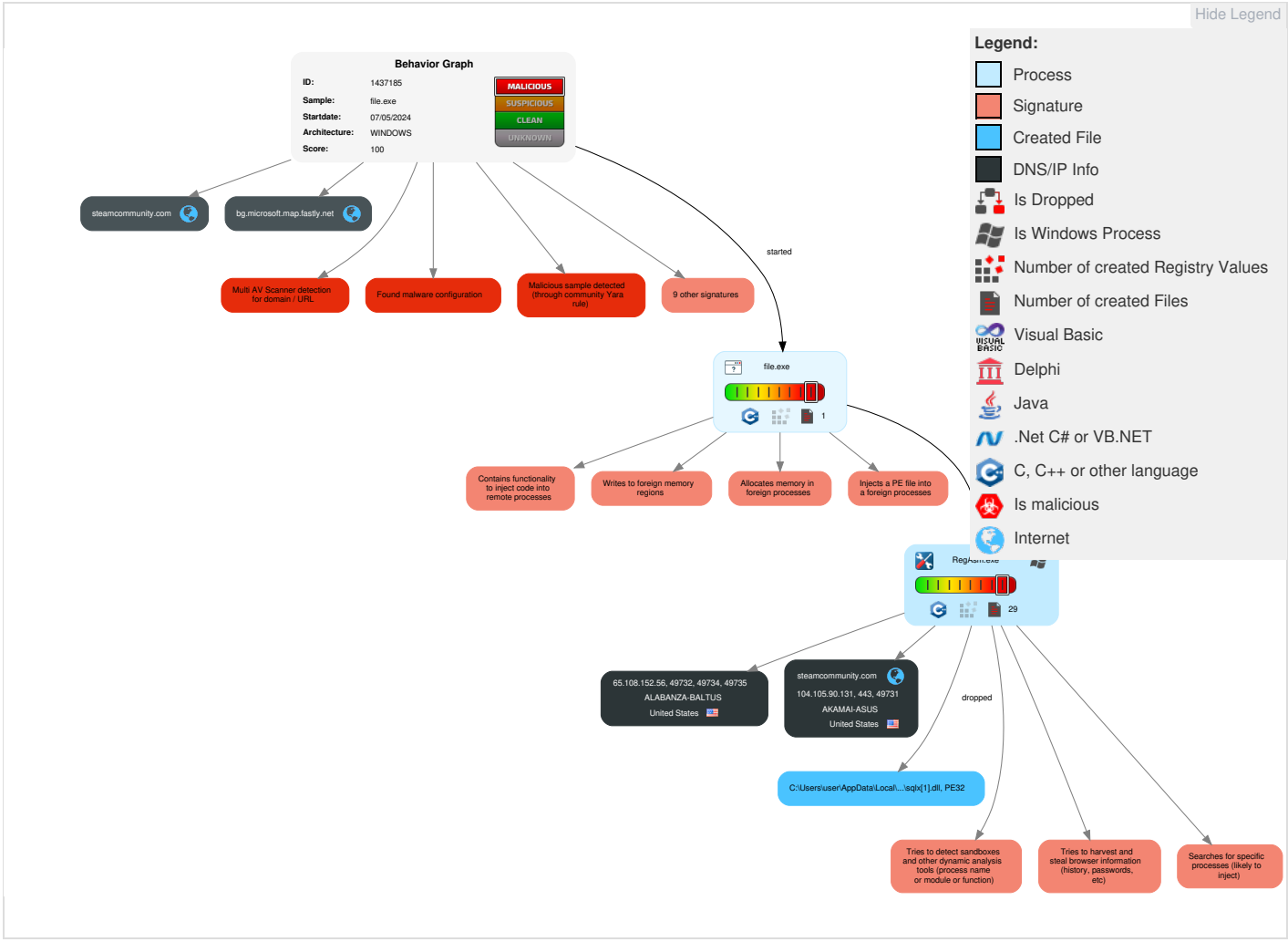
Yara detected PureLog Stealer

Yara detected Vidar stealer

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	Boot or Logon Initialization Scripts	5 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	2 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	1 Non-Standard Port	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 2 Software Packing	NTDS	4 4 System Information 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 4 1 Security Software 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 Masquerading	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	3 1 Virtualization/Sandbox Evasion	DCSync	1 2 Process Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	5 1 1 Process Injection	Proc Filesystem	1 System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

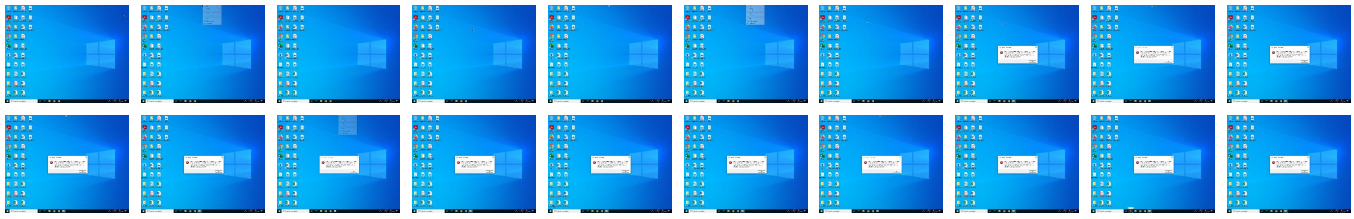
Behavior Graph

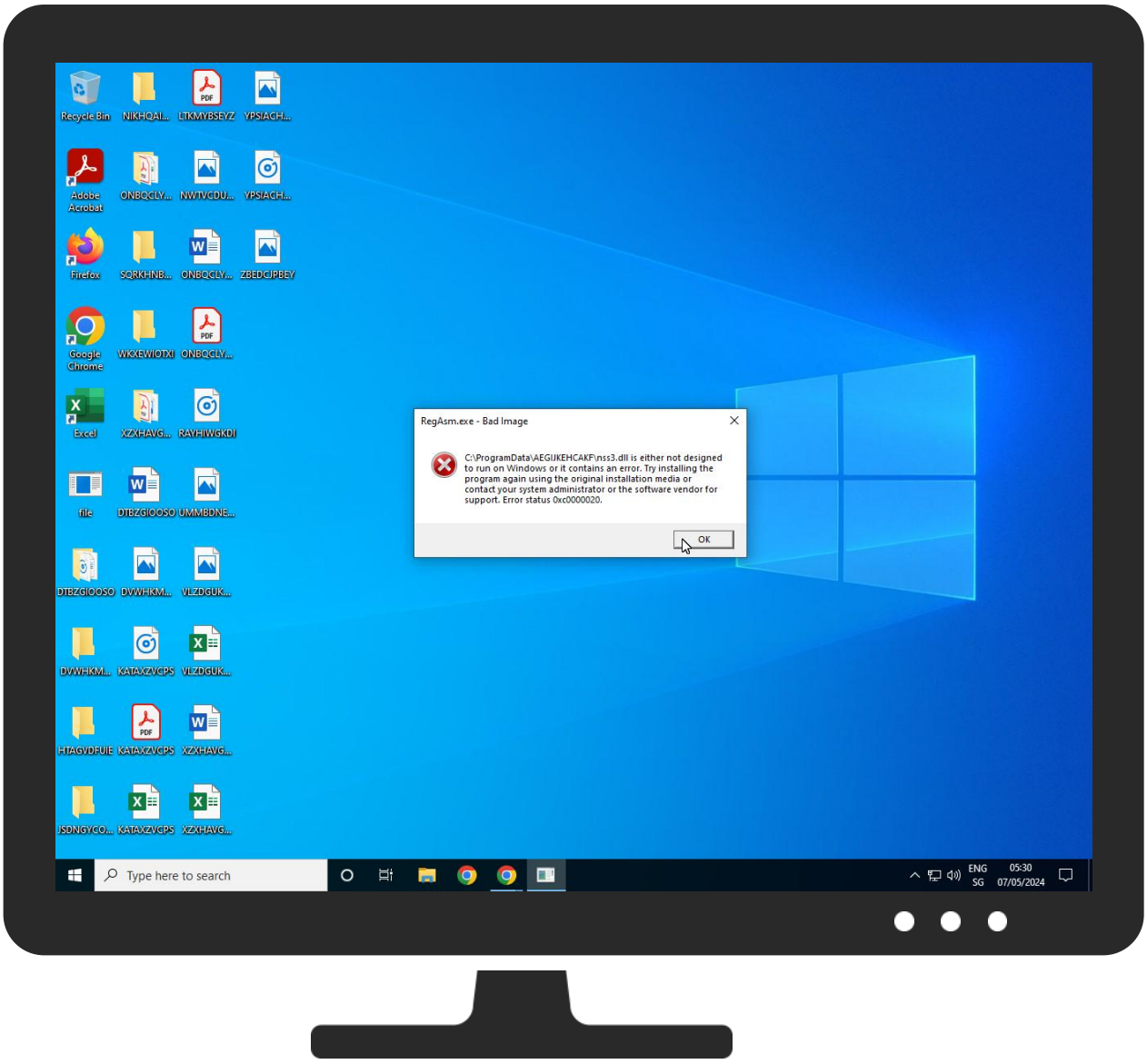


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	63%	ReversingLabs	Win32.Trojan.Privateloader	
file.exe	42%	Virustotal		Browse
file.exe	100%	Avira	HEUR/AGEN.1323756	
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		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	1%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bg.microsoft.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://65.108.152.56:9000/nss3.dllData	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/mozglue.dll	0%	Avira URL Cloud	safe	
http://https://store.steampowered.comv	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/nss3.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/nss3.dllft	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/softokn3.dllessionKeyBackward	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/nss3.dllU	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/freebl3.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000el	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/o	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/W	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/msvcp140.dllt	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000	0%	Virustotal		Browse
http://https://65.108.152.56:9000/G	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/D	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/soft	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/softokn3.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000softokn3.dlldge	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/7	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/dZ	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/W	9%	Virustotal		Browse
http://https://65.108.152.56:9000/mozglue.dllEdge	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000ing	0%	Avira URL Cloud	safe	
http://https://65.108.152.56/	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/sqlx.dllg	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/vcruntime140.dll_7)	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000lGoogle	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/	0%	Virustotal		Browse
http://https://65.108.152.56:9000/freebl3.dll4	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000l	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/ng	0%	Avira URL Cloud	safe	
http://https://65.108.152.56/	0%	Virustotal		Browse
http://https://65.108.152.56:9000/msvcp140.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/D	7%	Virustotal		Browse
http://https://65.108.152.56:9000e1a3fmium	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/L~	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/sqlx.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/sqlx.dllg	9%	Virustotal		Browse
http://https://65.108.152.56:9000/sqlx.dll	4%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bg.microsoft.map.fastly.net	199.232.210.172	true	false	• 0%, Virustotal, Browse	unknown
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	IEHJJE.1.dr	false		high
http://https://duckduckgo.com/ac/?q=	IEHJJE.1.dr	false		high
http://https://steamcommunity.com/?subsection=broadcasts	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/shared_global.js?v=wJD9maDpDcV	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://store.steampowered.comv	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/mozglue.dll	RegAsm.exe, 00000001.00000002.2881273063.0000000000E4B000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000	76561199680449169[1].htm.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/vcruntime140.dll	RegAsm.exe, 00000001.00000002.2881326562.0000000000EA4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=engli	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/javascript/promo/stickers.js?v=GfA42_x2_aub&	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/nss3.dllData	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpE	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://www.valvesoftware.com/legal.htm	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/main.js?v=roSu	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	RegAsm.exe, 00000001.00000002.2880201060.0000000000573000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://65.108.152.56:9000/nss3.dll	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2881326562.0000000000EA4000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://65.108.152.56:9000/nss3.dllft	RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/softokn3.dllessionKeyBackward	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/nss3.dllU	RegAsm.exe, 00000001.00000002.2881415199.0000000000F95000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000el	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh&	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/freebl3.dll	RegAsm.exe, 00000001.00000002.2881273063.0000000000E4B000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2881326562.0000000000EA4000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/javascript/modalContent.js?v=Wd0kCESeJquW&l=	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw&	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/o	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/css/applications/community/main.css?v=tIrWyaxi8A	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/shared/css/shared_responsive.css?v=eghn9DNyCY67&	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://store.steampowered.com/points/shop/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	IEHJJE.1.dr	false		high
http://https://65.108.152.56:9000/W	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	RegAsm.exe, 00000001.00000002.2880201060.0000000000573000.00000040.00000400.00020000.00000000.sdmp, HDBKJE.1.dr	false		high

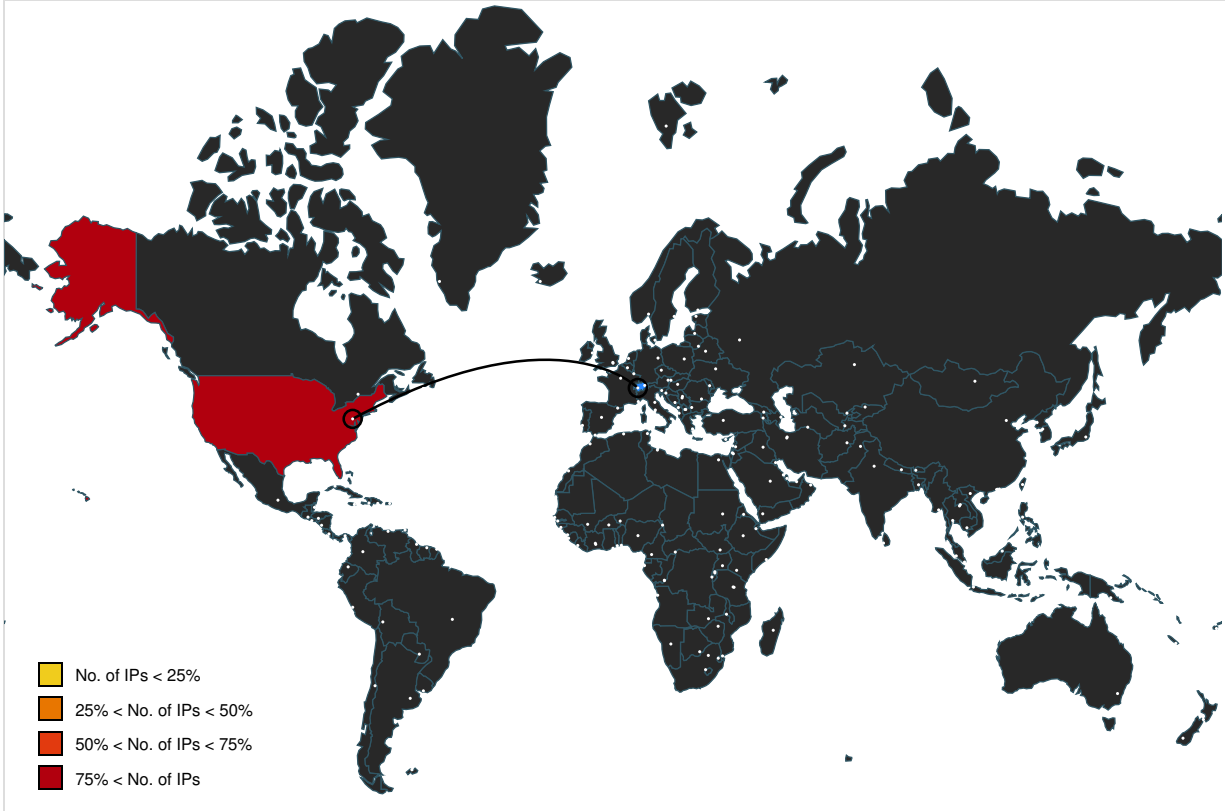
Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://community.cloudflare.steamstatic.com/public/css/promo/summer2017/stickers.css?v=bZKSp7oNwVPK	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http:// https://community.cloudflare.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http:// https://steamcommunity.com/profiles/76561199680449169/badges	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://www.ecosia.org/newtab/	IEHJJE.1.dr	false		high
http://https://65.108.152.56:9000/msvcp140.dllt	RegAsm.exe, 00000001.00000002.2881273063.0000000000E4B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://store.steampowered.com/privacy_agreement/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http:// https://community.cloudflare.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/G	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/D	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://community.cloudflare.steamstatic.com/public/shared/css/shared_global.css?v=2VoZa2M8Wh3k&	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http:// https://community.cloudflare.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/soft	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/softokn3.dll	RegAsm.exe, 00000001.00000002.2881273063.0000000000E4B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000softokn3.dlldge	RegAsm.exe, 00000001.00000002.2880201060.0000000000573000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// https://community.cloudflare.steamstatic.com/public/javascript/applications/community/libraries~b28b	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/	RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/7	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://community.cloudflare.steamstatic.com/public/shared/images/responsive/header_logo.png	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://65.108.152.56:9000/dZ	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/mozglue.dllEdge	RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	HDBKJE.1.dr	false		high
http://https://65.108.152.56:9000ing	RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://store.steampowered.com/about/	76561199680449169[1].htm.1.dr	false		high
http://https://steamcommunity.com/my/wishlist/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC&	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56/	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/sqlx.dllg	RegAsm.exe, 00000001.00000002.2881415199.0000000000F95000.00000004.00000020.00020000.00000000.sdmp	false	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/vcruntime140.dll_7)	RegAsm.exe, 00000001.00000002.2880201060.0000000000573000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://help.steampowered.com/en/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://steamcommunity.com/market/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://store.steampowered.com/news/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/toolt	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://community.cloudflare.steamstatic.com/public/javascript/global.js?v=PyuRtGtUpR0t&l=englis	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	IEHJJE.1.dr	false		high
http://store.steampowered.com/subscriber_agreement/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199680449169	76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/javascript/applications/community/manifest.js?v=	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	RegAsm.exe, 00000001.00000002.2880201060.0000000000573000.00000040.00000400.00020000.00000000.sdmp, HDBKJE.1.dr	false		high
http://https://steamcommunity.com/discussions/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://t.me/r1g1o	file.exe, 00000000.00000002.1632108400.000000003D65000.00000004.00000800.00020000.00000000.sdmp, RegAsm.exe, RegAsm.exe, 00000001.00000002.2880201060.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://store.steampowered.com/stats/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0&	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000lGoogle	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://store.steampowered.com/steam_refunds/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/images/skin_1/arrowDn9x5.gif	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/freebl3.dll4	RegAsm.exe, 00000001.00000002.2881326562.0000000000EA4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	HDBKJE.1.dr	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	IEHJJE.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.p	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000l	RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://65.108.152.56:9000/ng	RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/msvcp140.dll	RegAsm.exe, 00000001.00000002.2881273063.0000000000E4B000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880201060.0000000000535000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000e1a3fmium	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity.com/workshop/	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://store.steampowered.com/legal/	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://65.108.152.56:9000/L~	RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.cloudflare.steamstatic.com/public/shared/images/r	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000001.00000002.2886655892.000000001B6DD000.00000002.00001000.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2882085104.0000000015737000.00000004.00000020.00020000.00000000.sdmp, sqlx[1].dll.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/shared/css/buttons.css?v=tuNiaSwXwcYT&l=engl	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/shared/css/motiva_sans.css?v=GfSjbGKcNYaQ&l=	76561199680449169[1].htm.1.dr	false		high
http://https://community.cloudflare.steamstatic.com/public/css/skin_1/profilev2.css?v=gNE3gksLVEVa&l=en	RegAsm.exe, 00000001.00000002.2880201060.000000000043C000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000001.00000002.2880922498.0000000000DBD000.00000004.00000020.00020000.00000000.sdmp, 76561199680449169[1].htm.1.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	IEHJJE.1.dr	false		high
http://https://65.108.152.56:9000/sqlx.dll	RegAsm.exe, 00000001.00000002.2880201060.000000000052F000.00000040.00000400.00020000.00000000.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.108.152.56	unknown	United States		11022	ALABANZA-BALTUS	false
104.105.90.131	steamcommunity.com	United States		16625	AKAMAI-ASUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1437185
Start date and time:	2024-05-07 05:28:06 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 19s
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@3/12@1/2
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 199.232.210.172, 104.102.251.17, 104.102.251.89
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com.delivery.microsoft.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-b-net.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, download.windowsupdate.com.edgesuite.net
- 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
05:28:58	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\AEGIJKEHCAKF\BKKFHI

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\AEGIJKEHCAKF\GDBAKK

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\AEGIJKEHCAKF\GHJJDG	
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\AEGIJKEHCAKF\GHJKEH	
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\AEGIJKEHCAKF\HDBKJE	
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\AEGIJKEHCAKF\IEHJJE

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\ProgramData\AEGIJKEHCAKF\KFIJEG

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

C:\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+AOQOXl0Usvwr:feRG6BX6gUaHo9tkBHiUewr
MD5:	29F65BA8E88C063813CC50A4EA544E93
SHA1:	05A7040D5C127E68C25D81CC51271FFB8BEF3568
SHA-256:	1ED81FA8DFB6999A9FEDC6E779138FFD99568992E22D300ACD181A6D2C8DE184
SHA-512:	E29B2E92C496245BED3372578074407E8EF8882906CE10C35B3C8DEEBFEFE01B5FD7F3030ACAA693E175F4B7ACA6CD7D8D10AE1C731B09C5FA19035E005DE3AA
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,\.$.n.Q.\.p...R..:.hr./..8.S<a.s...+#3....D..h1.a.0....{.9.....:e.....n.~G.{.M.1..OU.....B.Q..y_>.P{...}i.=.a..QQT.U..\|!.pyCD@.....I..70..w..)...W^.`I...%Y.\.....i..=hYV.O8W@P.=.r.=..1m..1....)\.p..\|.c.3..t..[...).....I.{.Y....\S.....y....[.mCt....Js;...H....Q..F.....g.O...[..A.=...F[..z....k...mo.IW{`....O...T.g.Y.Uh.;m.'.N..f..}4..9i..t4p_bl..`.....Ie..I.P.... ...Lg.....[....5g...~D.s.h'>n.m.c.7...-..P.gG...i$...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):	3.217935332070547
Encrypted:	false
SSDEEP:	6:kKklEN+SkQlPlEGYRMY9z+4KlDA3RUeVlWI/Vt:MlbkPlE99SNxAhUeVLVt
MD5:	457C16EABAD85393C2438B34FEB507A6
SHA1:	0CE6ADD73AD8EE9C5AE93913F90C10F60B2E2F84
SHA-256:	DA40515D3E2FB4633893866C996982458B76FFDA1977689597DAED2146E26A71
SHA-512:	D9FA070DE00C0BDDE916FD8A902302CFC9BC09FFCC0BFAAC8CD967EA39A790DB8D85905176ECBC09E2F1DF19749D8FD9D113AE2D7F46DC3350B96FB1B329389
Malicious:	false
Preview:	p..... ..... .9.....(..... ....M.....(.....wl....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\CLR_v4.0_32\UsageLogs\file.exe.log

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177CE
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

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 (3041), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	35663
Entropy (8bit):	5.3820204547725865
Encrypted:	false
SSDEEP:	768:c7pqLtWYmwt5D0gq9siNGAGPzzgiJmDzJtxvrfukPco1AUmPzzgiJmDzJtxvJ2Sq:c78LtWYmwt5D0gq9scGPzzgiJmDzJtx2
MD5:	ED01FF8187C1C331702AB5F6E5E1631B
SHA1:	B982DE4E0762387C0FFFCFAC84B86FAE16EA52C1
SHA-256:	CB3DC06E3EBE65FC84FB78704A23A69B5961B6F62D72CAD01B2AECD4774763BE
SHA-512:	3CCFEF284D9A104BCC00BDE50CAC1DE5578281BFF2F8DA1872AC722E128C5814CD4B77438BB80577E825BE077A8426FB2629995D905C5D03847E56D0ECC01C9
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://65.108.152.56:9000|</title>...<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">.....<link href="https://community.cloudflare.steamstatic.com/public/shared/css/motiva_sans.css?v=GfSjbGKcNYaQ&l=english&_cdn=cloudflare" rel="stylesheet" type="text/css" >.<link href="https://community.cloudflare.steamstatic.com/public/shared/css/buttons.css?v=tuNiaSwXwcYT&l=english&_cdn=cloudflare" rel="stylesheet" type="text/css" >.<link href="https://community.cloudflare.steamstatic.com/public/shared/css/shared_global.css?v=2VoZa2M8Wh3k&l=english&_cdn=cloudflare" rel="stylesheet" type="text/css" >.<link href="https://community.cloudflare.steamstatic.com/public/css/global

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2459136
Entropy (8bit):	6.052474106868353

Encrypted:	false
SSDEEP:	49152:WHoJ9zGioiMjW2RrL9B8SSpiCH7cuez9A:WHoJBGqabRnj8JY/9
MD5:	90E744829865D57082A7F452EDC90DE5
SHA1:	833B178775F39675FA4E55EAB1032353514E1052
SHA-256:	036A57102385D7F0D7B2DEACF932C1C372AE30D924365B7A88F8A26657DD7550
SHA-512:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E57032 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.Z.Y.Z.Y.Z.Y...Z.n.Y...\..Y...]...Y...X.Y.Y.Z.X..Y.O.\.E.Y. O.].U.Y.O.Z.L.Y.l3].[.Y.l3Y.[.Y.l3..[.Y.l3[.[.Y.RichZ.Y.....PE..L...i.`e.....!...%.. .....{D..... .....%.....@.....#..6....$.(.....$..... .....$....`.#.8.....x.#.@.....$.....text...G. ....`.rdata..."..... ..$.... .....@..@.data...4|... $..b....#.....@....idata.... ....$.....^$.....@..@.00cfg.....$.....p$.....@..@.rsrc.....$.....r$.....@..@.reloc..5.....$.....$.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.414407050048219
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	358'000 bytes
MD5:	b9773393891d9cc471cd58cac09052dd
SHA1:	784a14954c7abca7d7e2e92c60b93557238426f4
SHA256:	0a8357cb9a1d348d1c4b4ec101f2328fd43f976803bcc360525ced55fbb9aeaf
SHA512:	72a669e736ecfc5422a07542e15cad7d82b9ae41591f4c375e31fa4dc2d70f620b44ff19b5b6d0928aac3cf244a3143af433d47eeaa3c5c6b9968cf71d1e6848
SSDEEP:	6144:Dqv0lb3JJzx1MfjF+N33l3+YBVYjZ7eZH9PJWweK/ojy8Kkc2ivFt+0P:Gb3TEbF+13NPYd6B9lcdFBsPP
TLSH:	B1749FD48267CF37D3ED0778F095120593FD820B8893FB4A6A2416A1590A3E2F7566FB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o.8f.....F.....d... .....@.. .....`

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x4564de
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6638D46F [Mon May 6 13:00:31 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4

Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 08/10/2020 01:00:00 12/10/2023 13:00:00
Subject Chain	• CN=ASUSTeK COMPUTER INC., O=ASUSTeK COMPUTER INC., L=Beitou District, S=Taipei City, C=TW, SERIALNUMBER=23638777, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=TW
Version:	3
Thumbprint MD5:	332CDC164B1324C3FF3F64E228C5FFFC
Thumbprint SHA-1:	CBFB3D25134A5FF6FCF2924D5B4BE16194EA7E13
Thumbprint SHA-256:	531855F05B9D55E4F6DDEBC443706382DDB9ACBD2B8AB24004822BE204420943
Serial:	0C9838F673F9B1CCE395CFAB2B6684E4

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x56490	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x58000	0x53c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x55000	0x2670	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x56447	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x544e4	0x54600	cd200369f3723ebffd9769e4598cb5e7	False	0.7394241898148148	data	7.421157543801175	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x58000	0x53c	0x600	b3903f7a2f10b94867e427ae266651a6	False	0.390625	data	3.9246143706878946	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5a000	0xc	0x200	fb9aeb40bfad98519cace1adb7b9f6da	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

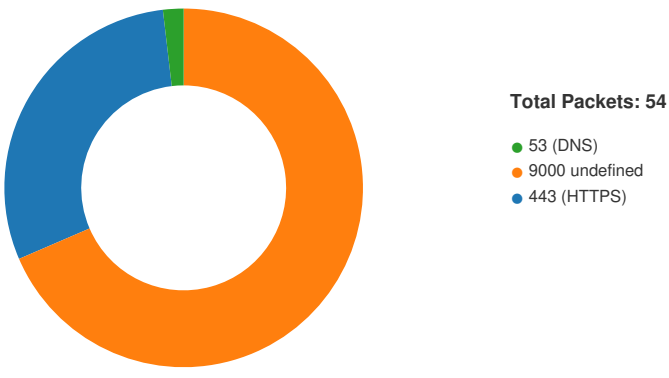
Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_VERSION	0x580a0	0x2b0	data			0.4375
RT_MANIFEST	0x58350	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5469387755102041

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2024 05:28:54.186081886 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.186120033 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.186193943 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.192341089 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.192354918 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.373563051 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.373641014 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.444263935 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.444284916 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.444617987 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.444678068 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.447978020 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.488120079 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.825839996 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.825865030 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.825894117 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.825948954 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.825969934 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.825989008 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.826020956 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.911032915 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.911071062 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.911122084 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.911129951 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.911159992 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.911175013 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.929805040 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.929846048 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.929867983 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.929883003 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.929925919 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.930380106 CEST	49731	443	192.168.2.4	104.105.90.131
May 7, 2024 05:28:54.930394888 CEST	443	49731	104.105.90.131	192.168.2.4
May 7, 2024 05:28:54.940658092 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:55.124442101 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:55.124541044 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:55.124906063 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:55.308558941 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:55.335064888 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:55.335078001 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:55.335280895 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:55.904119015 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.088542938 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:56.088629007 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.088963985 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.314002037 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:56.604398012 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:56.604489088 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.607820034 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.791517973 CEST	9000	49734	65.108.152.56	192.168.2.4
May 7, 2024 05:28:56.791601896 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.791857958 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.975559950 CEST	9000	49734	65.108.152.56	192.168.2.4
May 7, 2024 05:28:56.975790024 CEST	9000	49734	65.108.152.56	192.168.2.4
May 7, 2024 05:28:56.975832939 CEST	49734	9000	192.168.2.4	65.108.152.56

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2024 05:28:56.976175070 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:56.977679014 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.161231041 CEST	9000	49734	65.108.152.56	192.168.2.4
May 7, 2024 05:28:57.567095041 CEST	9000	49734	65.108.152.56	192.168.2.4
May 7, 2024 05:28:57.567166090 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.568280935 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.568749905 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.752975941 CEST	9000	49732	65.108.152.56	192.168.2.4
May 7, 2024 05:28:57.753046989 CEST	49732	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.755163908 CEST	9000	49735	65.108.152.56	192.168.2.4
May 7, 2024 05:28:57.755229950 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.755485058 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.940929890 CEST	9000	49735	65.108.152.56	192.168.2.4
May 7, 2024 05:28:57.941137075 CEST	9000	49735	65.108.152.56	192.168.2.4
May 7, 2024 05:28:57.941189051 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.943748951 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:57.945174932 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.130691051 CEST	9000	49735	65.108.152.56	192.168.2.4
May 7, 2024 05:28:58.491302967 CEST	9000	49735	65.108.152.56	192.168.2.4
May 7, 2024 05:28:58.491322041 CEST	9000	49735	65.108.152.56	192.168.2.4
May 7, 2024 05:28:58.491475105 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.492830992 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.493206978 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.681381941 CEST	9000	49734	65.108.152.56	192.168.2.4
May 7, 2024 05:28:58.681405067 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:58.681457043 CEST	49734	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.681514978 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.681926966 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.865605116 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:58.865900040 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:58.865962982 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.866276026 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:58.867717028 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:59.053447008 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:59.444582939 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:59.444606066 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:59.444619894 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:59.444633961 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:59.444647074 CEST	9000	49736	65.108.152.56	192.168.2.4
May 7, 2024 05:28:59.444659948 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:59.444688082 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:59.444708109 CEST	49736	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:59.496557951 CEST	49735	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:59.496889114 CEST	49737	9000	192.168.2.4	65.108.152.56
May 7, 2024 05:28:59.682235956 CEST	9000	49735	65.108.152.56	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2024 05:28:54.095249891 CEST	55374	53	192.168.2.4	1.1.1.1
May 7, 2024 05:28:54.181236029 CEST	53	55374	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 7, 2024 05:28:54.095249891 CEST	192.168.2.4	1.1.1.1	0xa13a	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false

DNS Answers

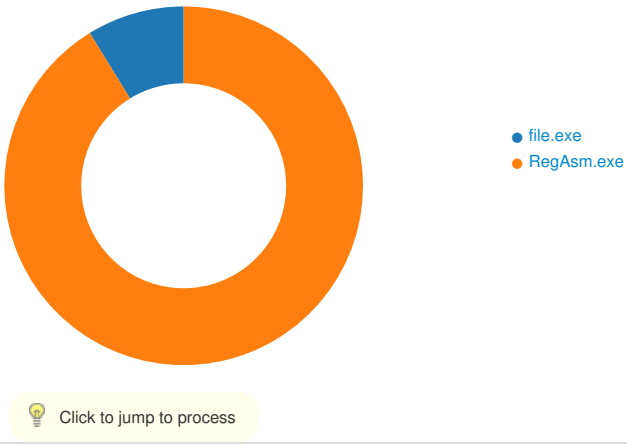
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 7, 2024 05:28:54.181236029 CEST	1.1.1.1	192.168.2.4	0xa13a	No error (0)	steamcommunity.com		104.105.90.131	A (IP address)	IN (0x0001)	false
May 7, 2024 05:28:55.456705093 CEST	1.1.1.1	192.168.2.4	0x10a7	No error (0)	bg.microsoft.map.fastly.net		199.232.210.172	A (IP address)	IN (0x0001)	false
May 7, 2024 05:28:55.456705093 CEST	1.1.1.1	192.168.2.4	0x10a7	No error (0)	bg.microsoft.map.fastly.net		199.232.214.172	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 3228, Parent PID: 2580

General

Target ID:	0
Start time:	05:28:52
Start date:	07/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x9a0000
File size:	358'000 bytes
MD5 hash:	B9773393891D9CC471CD58CAC09052DD
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: 00000000.00000002.1632108400.0000000003D65000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000000.1628578580.000000000009A2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7303A0B7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	0	42	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",1	success or wait	1	7303A147	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B60842	ReadFile

Analysis Process: RegAsm.exe PID: **5816**, Parent PID: **3228**

General

Target ID:	1
Start time:	05:28:52
Start date:	07/05/2024
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:	0x7e0000
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: 00000001.00000002.2880201060.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000001.00000002.2880201060.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	high
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\AEGIJKEHCAKF	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	415BA3	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40506B	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	40506B	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	40506B	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	40506B	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	40506B	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	40506B	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	40506B	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	40506B	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	40506B	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	40506B	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	40506B	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	40506B	HttpSendRequestA
C:\ProgramData\AEGIJKEHCAKF\GHJKEH	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	4068FA	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\AEGIJKEHCAKF\HDBKJE	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	40C260	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\KFIJEG	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	40B405	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\IEHJJE	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	40BFC7	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\BKKFHI	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	40C260	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\GHJJDG	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	40B405	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\GDBAKK	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	40BFC7	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EBA	CreateFileA
C:\ProgramData\AEGIJKEHCAKF\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EBA	CreateFileA
C:\ProgramData\AEGIJKEHCAKF\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EBA	CreateFileA
C:\ProgramData\AEGIJKEHCAKF\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EBA	CreateFileA
C:\ProgramData\AEGIJKEHCAKF\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EBA	CreateFileA
C:\ProgramData\AEGIJKEHCAKF\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404EBA	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\AEGIJKEHCAKF\GHJKEH	success or wait	1	406E11	DeleteFileA
C:\ProgramData\AEGIJKEHCAKF\HDBKJE	success or wait	1	40C356	DeleteFileA
C:\ProgramData\AEGIJKEHCAKF\KFIJEG	success or wait	1	40B6A3	DeleteFileA
C:\ProgramData\AEGIJKEHCAKF\IEHJJE	success or wait	1	40C147	DeleteFileA
C:\ProgramData\AEGIJKEHCAKF\BKKFHI	success or wait	1	40C356	DeleteFileA
C:\ProgramData\AEGIJKEHCAKF\GHJJDG	success or wait	1	40B6A3	DeleteFileA
C:\ProgramData\AEGIJKEHCAKF\GDBAKK	success or wait	1	40C147	DeleteFileA

File Written

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	40510F	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 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]YXYYZXYO\EYO]UYOZLYl3][Yl3Y[Yl3[Yl3[[YRichZY	success or wait	2291	40435F	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\AEGIJKEHCAKF\GHJKEH	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	SQLite format 3@ .jg$	success or wait	1	4068FA	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\HDBKJE	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	40C260	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\AEGIJKEHCAKF\KFIJEG	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	40B405	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\IEHJJE	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	40BFC7	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\AEGIJKEHCAKF\BKKFHI	0	126976	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40C260	CopyFileA
C:\ProgramData\AEGIJKEHCAKF\GHJJDG	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40B405	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\AEGIJKEHCAKF\GDBAKK	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 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	SQLite format 3@ 8$.O}4	success or wait	1	40BFC7	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	406252	ReadFile
C:\ProgramData\AEGIJKEHCAKF\GHJKEH	0	100	success or wait	6	1B49FE09	ReadFile
C:\ProgramData\AEGIJKEHCAKF\HDBKJE	0	100	success or wait	6	1B49FE09	ReadFile
C:\ProgramData\AEGIJKEHCAKF\HDBKJE	0	100	success or wait	6	1B49FE09	ReadFile
C:\ProgramData\AEGIJKEHCAKF\KFIJEG	0	100	success or wait	6	1B49FE09	ReadFile
C:\ProgramData\AEGIJKEHCAKF\IEHJJE	0	100	success or wait	27	1B49FE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	406252	ReadFile
C:\ProgramData\AEGIJKEHCAKF\BKKFHI	0	100	success or wait	12	1B49FE09	ReadFile
C:\ProgramData\AEGIJKEHCAKF\GHJJDG	0	100	success or wait	6	1B49FE09	ReadFile
C:\ProgramData\AEGIJKEHCAKF\GDBAKK	0	100	success or wait	20	1B49FE09	ReadFile

Disassembly

No disassembly