ID: 1453785
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:20:09
Date: 07/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

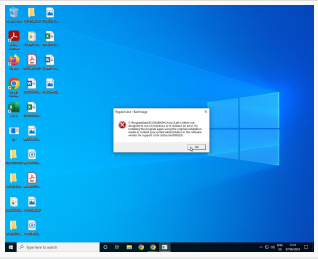
Windows Analysis Report

file.exe

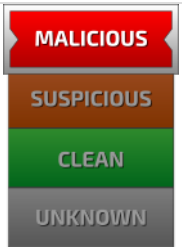
Overview

General Information

Sample name:	file.exe
Analysis ID:	1453785
MD5:	7dc8189f70cc3..
SHA1:	8cb698efdf597…
SHA256:	a3608a51db9d…
Tags:	exe
Infos:	



Detection



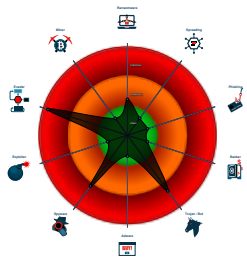
Vidar

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected Powershell download…
- Yara detected Vidar stealer
- AI detected suspicious sample
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Contains functionality to inject code…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6360 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 7DC8189F70CC34E18EA7AF8FDEAC4142)
  - RegAsm.exe (PID: 2780 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/76561199698764354",
    "https://t.me/r8z0l"
  ],
  "Botnet": "8bd2ac5f1dd228859ac690a79c0bde71"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.2070870185.0000000001023000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.3325415366.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.3325415366.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x231f0:$s1: JohnDoe • 0x231e8:$s2: HAL9TH
Process Memory Space: file.exe PID: 6360	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: file.exe PID: 6360	JoeSecurity_PowershellDownloadAndExecute	Yara detected Powershell download and execute	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.RegAsm.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x231f0:$s1: JohnDoe • 0x231e8:$s2: HAL9TH
2.2.RegAsm.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.RegAsm.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x225f0:$s1: JohnDoe • 0x225e8:$s2: HAL9TH
0.2.file.exe.ff0000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

AI detected suspicious sample

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Yara detected Powershell download and execute

Allocates memory in foreign processes

Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Searches for specific processes (likely to inject)

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Vidar stealer

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

Remote Access Functionality

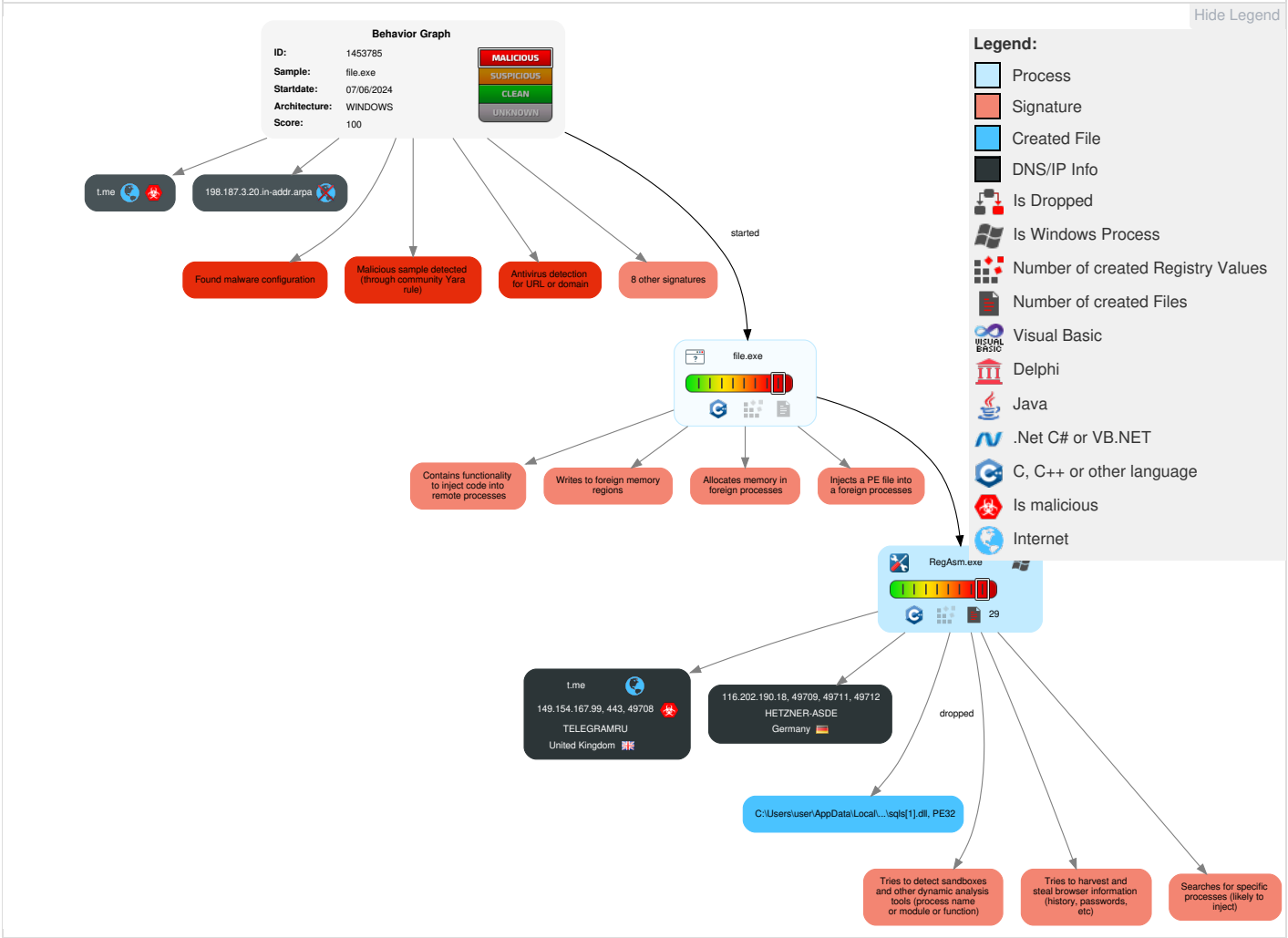
Yara detected Vidar stealer

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	5 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Screen Capture	2 1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	5 1 1 Process Injection	LSASS Memory	1 4 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service

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

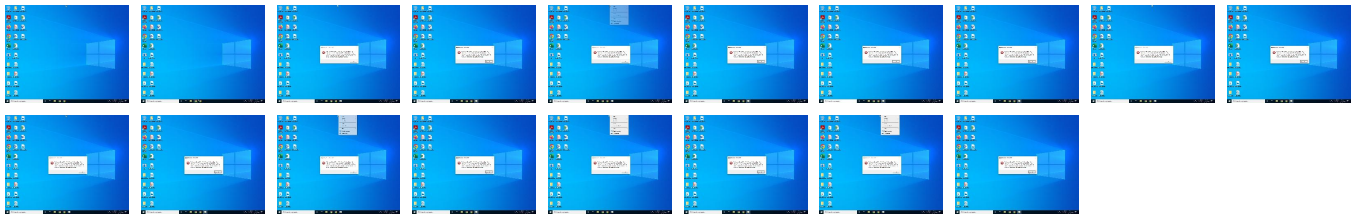
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	26%	ReversingLabs	Win32.Infostealer.Generic	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9C680Q69\sqls[1].dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432l	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/softokn3.dllP	100%	Avira URL Cloud	malware	
http://https://116.202.190.18/	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/softokn3.dll	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net02	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/msvcp140.dlldge	100%	Avira URL Cloud	malware	
http://https://web.telegram.org	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/vcruntime140.dllIQ=E	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/softokn3.dllZ	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432Content-Disposition:	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/freebl3.dllEdge	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/sqls.dll	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/freebl3.dlla	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/reebl3.dll	100%	Avira URL Cloud	malware	
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/mozglue.dllEdge	100%	Avira URL Cloud	malware	
http://https://t.me/r8z0l	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/freebl3.dll	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/vcruntime140.dll9	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/nss3.dll	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/mozglue.dlls	100%	Avira URL Cloud	malware	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/vcruntime140.dllser	100%	Avira URL Cloud	malware	
http://crl.entrust.net/ts1ca.crl0	0%	Avira URL Cloud	safe	
http://https://t.me/i	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/vcruntime140.dll/	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/sqls.dllx	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/vcruntime140.dll	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/	100%	Avira URL Cloud	malware	
http://www.sqlite.org/copyright.html.	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432fold	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/.190.18:5432/	100%	Avira URL Cloud	malware	
http://https://t.me/w	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/oft	100%	Avira URL Cloud	malware	
http://www.entrust.net/rpa03	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/My	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/nss3.dllO	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/mozglue.dll	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/softokn3.dllOMh	100%	Avira URL Cloud	malware	
http://aia.entrust.net/ts1-chain256.cer01	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432A	0%	Avira URL Cloud	safe	
http://https://www.ecosia.org/newtab/	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432ing	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/nss3.dllft	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/msvcp140.dll	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://116.202.190.18:5432/vcruntime140.dllUser	100%	Avira URL Cloud	malware	
http://https://ac.ecosia.org/autocomplete?q=	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432/ng	100%	Avira URL Cloud	malware	
http://https://116.202.190.18:5432/softokn3.dlldge	100%	Avira URL Cloud	malware	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	Avira URL Cloud	safe	
http://https://steamcommunity.com/profiles/76561199698764354	100%	Avira URL Cloud	malware	
http://https://www.entrust.net/rpa0	0%	Avira URL Cloud	safe	
http://crl.entrust.net/2048ca.crl0	0%	Avira URL Cloud	safe	
http://https://t.me/r8z0lF	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432AMicrosoft	0%	Avira URL Cloud	safe	
http://https://116.202.190.18:5432c84cgle	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t.me	149.154.167.99	true	true		unknown
198.187.3.20.in-addr.arpa	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://t.me/r8z0l	true	• Avira URL Cloud: malware	unknown
https://steamcommunity.com/profiles/76561199698764354	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

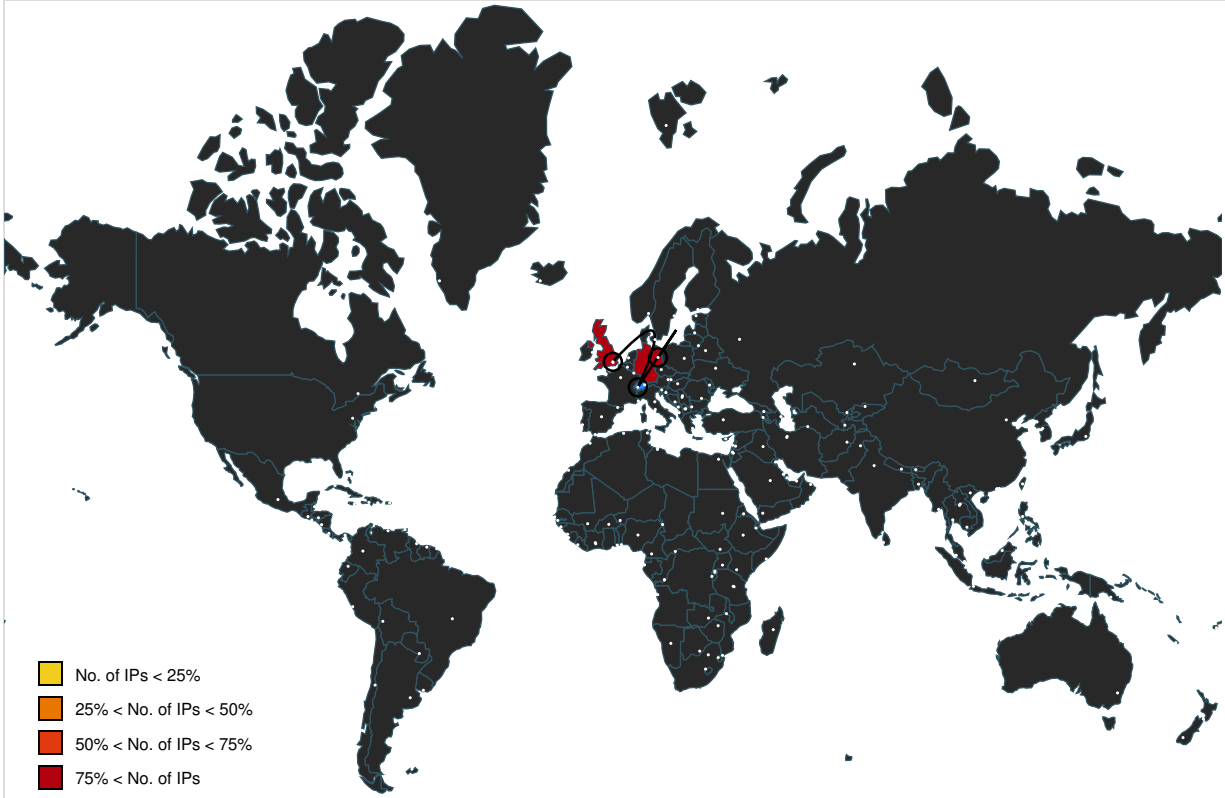
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://116.202.190.18/	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/chrome_newtab	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/softokn3.dllP	RegAsm.exe, 00000002.00000002.3326524144.0000000001280000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432l	RegAsm.exe, 00000002.00000002.3325415366.0000000000453000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://web.telegram.org	RegAsm.exe, 00000002.00000002.3325415366.0000000000453000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326265923.0000000001193000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/msvcp140.dlldge	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net03	file.exe	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net02	file.exe	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/softokn3.dll	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326524144.0000000001280000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/vcruntime140.dllIQ=E	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/freebl3.dllEdge	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://116.202.190.18:5432/freebl3.dlla	RegAsm.exe, 00000002.00000002.3326524144.000000000129E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432Content-Disposition:	RegAsm.exe, 00000002.00000002.3325415366.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/sqls.dll	RegAsm.exe, 00000002.00000002.3325415366.0000000000491000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326524144.000000000129E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/reebl3.dll	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/softokn3.dllZ	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/mozglue.dllEdge	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/freebl3.dll	RegAsm.exe, 00000002.00000002.3326524144.000000000129E000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/vcruntime140.dll9	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/mozglue.dlls	RegAsm.exe, 00000002.00000002.3326524144.000000000129E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/nss3.dll	RegAsm.exe, 00000002.00000002.3326265923.00000000011C9000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326524144.000000000129E000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/vcruntime140.dll/	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/vcruntime140.dllser	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://t.me/i	RegAsm.exe, 00000002.00000002.3326265923.000000000113A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/ts1ca.crl0	file.exe	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/sqls.dllx	RegAsm.exe, 00000002.00000002.3326524144.000000000129E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/vcruntime140.dll	RegAsm.exe, 00000002.00000002.3326524144.0000000001268000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3325415366.000000000056E000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432	RegAsm.exe, 00000002.00000002.3326265923.0000000001193000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000002.00000002.3331463797.000000001B8CD000.00000002.00001000.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3327352173.0000000015922000.00000004.00000020.00020000.00000000.sdmp, sqls[1].dll.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://116.202.190.18:5432/	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326684704.0000000001397000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326265923.0000000001193000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432fold	RegAsm.exe, 00000002.00000002.3325415366.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/.190.18:5432/	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://t.me/w	RegAsm.exe, 00000002.00000002.3326265923.000000000113A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/oft	RegAsm.exe, 00000002.00000002.3326444422.00000000011EC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.entrust.net/rpa03	file.exe	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/nss3.dllO	RegAsm.exe, 00000002.00000002.3326684704.0000000001397000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/My	RegAsm.exe, 00000002.00000002.3326684704.0000000001397000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/softokn3.dllOMh	RegAsm.exe, 00000002.00000002.3326524144.0000000001280000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/mozglue.dll	RegAsm.exe, 00000002.00000002.3326524144.000000000129E000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://aia.entrust.net/ts1-chain256.cer01	file.exe	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432A	RegAsm.exe, 00000002.00000002.3325415366.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432ing	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/msvcp140.dll	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000002.00000002.3326524144.0000000001280000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/nss3.dllft	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/vcruntime140.dllUser	RegAsm.exe, 00000002.00000002.3325415366.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ac.ecosia.org/autocomplete?q=	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432/ng	RegAsm.exe, 00000002.00000002.3326684704.0000000001397000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://116.202.190.18:5432/softokn3.dlldge	RegAsm.exe, 00000002.00000002.3325415366.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	FBKECF.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://t.me/r8z0lF	RegAsm.exe, 00000002.00000002.3326265923.0000000001193000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	file.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.entrust.net/rpa0	file.exe	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432AMicrosoft	RegAsm.exe, 00000002.00000002.3325415366.0000000000497000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://116.202.190.18:5432c84cgle	RegAsm.exe, 00000002.00000002.3325415366.00000000004B6000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
116.202.190.18	unknown	Germany		24940	HETZNER-ASDE	false
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1453785
Start date and time:	2024-06-07 17:20:09 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 6m 3s
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:	6
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@3/11@2/2
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): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240
- 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
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
11:21:13	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\ECGHJJEHDHCA\BFCGDA	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\ProgramData\ECGHJJEHDHCA\BGDGHJ	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UlYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+Ul3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC00
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\ProgramData\ECGHJJEHDHCA\DBKKFC	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8439810553697228
Encrypted:	false
SSDEEP:	24:TLyAF1kwNbXYFpFNYcw+6UwcQVXH5fBO9p7n52GmCWGf+dyMDCFVE1:TeAFawNLopFgU10XJBOB2Gbf+ba+
MD5:	9D46F142BBCF25D0D495FF1F3A7609D3
SHA1:	629BD8CD800F9D5B078B5779654F7CBFA96D4D4E
SHA-256:	C11B443A512184E82D670BA6F7886E98B03C27CC7A3CEB1D20AD23FCA1DE57DA
SHA-512:	AC90306667AFD38F73F6017543BDBB0B359D79740FA266F587792A94FDD35B54CCE5F6D85D5F6CB7F4344BEDAD9194769ABB3864AAE7D94B4FD6748C31250A02
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\ProgramData\ECGHJJEHDHCA\EBGDHJ	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j...$.....g..... ....

C:\ProgramData\ECGHJJEHDHCA\FBKECF

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\ProgramData\ECGHJJEHDHCA\HJJKFB

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:\ProgramData\ECGHJJEHDHCA\IDAEHC

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988

Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7lwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\ProgramData\ECGHJJEHDHCA\JEHIID

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	modified
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\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, 71954 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	71954
Entropy (8bit):	**7.996617769952133**
Encrypted:	**true**
SSDEEP:	1536:gc257bHnClJ3v5mnAQEBP+bfnW8Ctl8G1G4eu76NWDdB34w18R5cBWcJAm68+Q:gp2ld5jPqW8LgeulxB3fgcEfDQ
MD5:	49AEBF8CBD62D92AC215B2923FB1B9F5
SHA1:	1723BE06719828DDA65AD804298D0431F6AFF976
SHA-256:	B33EFCB95235B98B48508E019AFA4B7655E80CF071DEFABD8B2123FC8B29307F
SHA-512:	BF86116B015FB56709516D686E168E7C9C68365136231CC51D0B6542AE95323A71D2C7ACEC84AAD7DCECC2E410843F6D82A0A6D51B9ACFC721A9C84FDD877E 5B
Malicious:	false
Preview:	MSCF.....,.....I.....XaK .authroot.stl.[.i..6..CK..<Tk.....4.cl!Kg..E..*Y.f_..".$mR"$.J.E.KB."..rKv.."{.g....3.W.....c..9.s...=....y6#..x.....D.....\(.#.s.!.A. .....cd.c.....+^.ov...n.....3BL..0.....BPUR&.X..02.q...R...J.....w.....b.vy>....-.&..(..oe."."...J9...0U.6J..|U..S.....M.F8g...=.....p.....l.?3.J.x.G.Ep..$g..tj.....)v]9(:.)W. 8.Op.1Q..:.nPd.....7.7..M].V F..g.....12..!7(...B.....h.RZ.....l.<.....6..Z^.`p?... .p.Gp.#.'.X.....|!.8.....".m.49r?.I...g...8.v.....a``.g.R4.i...J8q....NFW,E.6Y....!.o5%.Y.....R.. <..S9....r....WO...(.....F..Q=*....-..7d..O(....-..+k.....K.....{Q....Z..j._.E...QZ.~.\.^.....N.9.k..O.}dD.b1r...[}/....T..E..G..c.|.c.&>?..^t. ..;..X.d.E.0G....[Q.*,*.....#.Dp..L.o|#syc .J.....}G-.ou6.=52..XWi=...m.....^u.....c..fc?&pR7S5....l...j.G.....j.j..Tc.El....B.pQ.,Bp....j...9g.. >..s..m#.Nb.o_u.M.V.....\#...v..Mo\sF..s....Y...

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):	328
Entropy (8bit):	3.137989037915285
Encrypted:	false
SSDEEP:	6:kKPGT9UswDLL+N+SkQlPlEGYRMY9z+4KlDA3RUebT3:2qDnLNkPlE99SNxAhUe/3
MD5:	E113C02773BE81D3C280B225C06A3655
SHA1:	F01C16E165703E9F97C726AECF2CE956CAB2C3D9
SHA-256:	5D7D8A8AE4AFA4CC5872303C20186CC1DF574E75A323D9DD2AC9A6AD47AED049

SHA-512:	EDAD37963070E6E6BA6DF20075FB4DF28411911D4CAB10834DEA1A33DF7B8AAC5D8E3909323E97377D8CB1F04095476CC7675B73052C4C1CD4F0DC8A9F8704 0
Malicious:	false
Preview:	p..... .....V\VQ...(..... .....G..@.....&.....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...".a.7.2.8.2.e.b.4.0.b.1.d.a.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9C680Q69\sqls[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2459136
Entropy (8bit):	6.052474106868353
Encrypted:	false
SSDEEP:	49152:WHoJ9zGioiMjW2RrL9B8SSpiCH7cuez9A:WHoJBGqabRnj8JY/9
MD5:	90E744829865D57082A7F452EDC90DE5
SHA1:	833B178775F39675FA4E55EAB1032353514E1052
SHA-256:	036A57102385D7F0D7B2DEACF932C1C372AE30D924365B7A88F8A26657DD7550
SHA-512:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E57032 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.Z.Y.Z.Y.Z.Y...Z.n.Y...\..Y...]...Y...X.Y.Y.Z.X..Y.O.\.E.Y. O.].U.Y.O.Z.L.Y.l3].[.Y.l3Y.[.Y.l3..[.Y.l3[.[.Y.RichZ.Y.....PE..L...i.`e.....!...%.. .....{D..... .....%.....@.....#..6....$.(.....$..... .....$.....`.#.8.....x.#.@.....$.....text...G. ....`.rdata..."..... ..$.... .....@..@.data...4|... $..b....#.....@....idata.... ....$.....^$.....@..@.00cfg.....$.....p$.....@..@.rsrc.....$.....r$.....@..@.reloc..5.....$.....$.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.504017216084228
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:	442'408 bytes
MD5:	7dc8189f70cc34e18ea7af8fdeac4142
SHA1:	8cb698efdf5971e0805dd0f0fb0457315490c777
SHA256:	a3608a51db9df14c42f8c6e37ac49969de70b4be0862d82b5823c00aed395f9d
SHA512:	9bb17829724af371d383874b8ed4efe09f7f518fa131d68dd02ae0a149b0506f42b2694d7ec9a59b591b28fdcd620b68116e1170cd489b396d294126332e93ac
SSDEEP:	6144:+uvXVvZjkQbsWSHZhP2YQih4Qsc14gY8f4en6hZpG+es7SJnXZfGBTaDsj48bR4B:5vdkQbjcps2+8uhAs64TR47EO
TLSH:	9894E01275C08473EA6325324AF4D7B96A7DFC300EB2498FA3A51BBE4F342829721757
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T...T...T[..U...T[..U#..T[..U...TJi.U...T[..U...T...T...TJi.U...TJi.U...T{j.U...T{j.T...T{j.U...TRich...T.....

File Icon

Icon Hash:	00928e8e8686b000

Static PE Info

General

Entrypoint:	0x409caa
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x66630B74 [Fri Jun 7 13:30:28 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:	c746ee5ba8a06ab7dd2d5d1c7f055c1e

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 13/01/2023 01:00:00 17/01/2026 00:59:59
Subject Chain	• CN=NVIDIA Corporation, OU=2-J, O=NVIDIA Corporation, L=Santa Clara, S=California, C=US
Version:	3
Thumbprint MD5:	5F1B6B6C408DB2B4D60BAA489E9A0E5A
Thumbprint SHA-1:	15F760D82C79D22446CC7D4806540BF632B1E104
Thumbprint SHA-256:	28AF76241322F210DA473D9569EFF6F27124C4CA9F43933DA547E8D068B0A95D
Serial:	0997C56CAA59055394D9A9CDB8BEEB56

Entrypoint Preview
Instruction
call 00007F11211BEA47h
jmp 00007F11211BE0F9h
push ebp
mov ebp, esp
jmp 00007F11211BE28Fh
push dword ptr [ebp+08h]
call 00007F11211CA864h
pop ecx
test eax, eax
je 00007F11211BE291h
push dword ptr [ebp+08h]
call 00007F11211C54F9h
pop ecx
test eax, eax
je 00007F11211BE268h
pop ebp
ret
cmp dword ptr [ebp+08h], FFFFFFFFh
je 00007F11211B8AD2h
jmp 00007F11211BED36h
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call 00007F11211BED48h
pop ecx
pop ebp
ret
jmp 00007F11211BED40h
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi

Instruction
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007F11211BE29Bh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007F11211BE28Ch
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007F11211BE28Eh
add edx, 28h
cmp edx, esi
jne 00007F11211BE26Ch
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007F11211BE27Bh
push esi
call 00007F11211BECFBh
test eax, eax
je 00007F11211BE2A2h
mov eax, dword ptr fs:[00000018h]
mov esi, 004693ACh
mov edx, dword ptr [eax+04h]
jmp 00007F11211BE286h
cmp edx, eax
je 00007F11211BE292h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007F11211BE272h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+00h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x31d64	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6a000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x69a00	0x2628	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6b000	0x221c	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2f078	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x2f0c0	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2efb8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x27000	0x178	.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	0x2595b	0x25a00	d03b1ac577e8310a65cfcca0d1b9b28c	False	0.5770543500830565	data	6.629946953103711	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0xb638	0xb800	83ce0a9da3b5383dcb7ae371d186047b	False	0.4192000679347826	data	4.874082709437768	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x33000	0x36ebc	0x35e00	8c632b07301722aef05673ff6d2dbc3e	False	0.9738979118329466	data	7.979395809192078	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6a000	0x1e0	0x200	ec748486ad40c4e6cd2019b55b71ef97	False	0.53125	data	4.7176788329467545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6b000	0x221c	0x2400	f99ed12824f202033297dec3df069714	False	0.7098524305555556	data	6.4054305886337835	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_MANIFEST	0x6a060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.5931758530183727

Imports

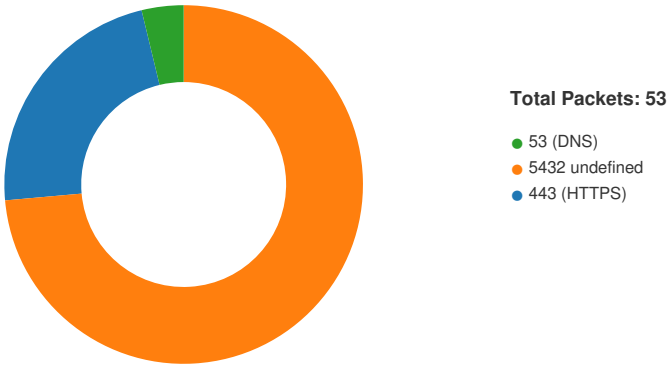
DLL	Import
ADVAPI32.dll	RegEnableReflectionKey, DeleteAce
KERNEL32.dll	WaitForSingleObjectEx, CreateThread, VirtualAlloc, GetModuleHandleA, GetProcAddress, RaiseException, InitOnceBeginInitialize, InitOnceComplete, ReleaseSRWLockExclusive, AcquireSRWLockExclusive, TryAcquireSRWLockExclusive, GetCurrentThreadId,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

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2024 17:21:04.529378891 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:04.529469967 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:04.529561996 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:04.549695969 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:04.549732924 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.423832893 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.424055099 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.467292070 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.467319012 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.468219042 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.468286037 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.473617077 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.520513058 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.787926912 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.787965059 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.788023949 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.788059950 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.788080931 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.788081884 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.788081884 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.788178921 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.798670053 CEST	49708	443	192.168.2.5	149.154.167.99
Jun 7, 2024 17:21:05.798715115 CEST	443	49708	149.154.167.99	192.168.2.5
Jun 7, 2024 17:21:05.824611902 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:05.829792976 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:05.830240965 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:05.830362082 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:05.835469961 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:06.702445030 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:06.702464104 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:06.702553988 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:07.904989958 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:07.909918070 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:08.151453018 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:08.151582003 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:08.152216911 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:08.157123089 CEST	5432	49709	116.202.190.18	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2024 17:21:08.654932022 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:08.655482054 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:08.660881996 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:08.665803909 CEST	5432	49711	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:08.665992022 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:08.666332006 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:08.671190023 CEST	5432	49711	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:09.512254000 CEST	5432	49711	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:09.512331009 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:09.512737989 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:09.515331984 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:09.517590046 CEST	5432	49711	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:09.520246029 CEST	5432	49711	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:10.054327965 CEST	5432	49711	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:10.054414988 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.069391966 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.070051908 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.074610949 CEST	5432	49709	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:10.074702024 CEST	49709	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.075190067 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:10.075259924 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.075542927 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.080343008 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:10.923140049 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:10.923269033 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.923600912 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.925312042 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:10.928489923 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:10.930213928 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:11.455221891 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:11.455261946 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:11.455355883 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:11.457024097 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:11.457264900 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:11.462129116 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:11.462217093 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:11.462248087 CEST	5432	49711	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:11.462414980 CEST	49711	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:11.462449074 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:11.467353106 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.323450089 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.323539972 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.324070930 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.326373100 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.329113960 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.331222057 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.866233110 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.866247892 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.866254091 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.866333961 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.866343975 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.866353035 CEST	5432	49713	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.866370916 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.866432905 CEST	49713	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.868168116 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.868549109 CEST	49714	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.873472929 CEST	5432	49714	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.873521090 CEST	5432	49712	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:12.873583078 CEST	49714	5432	192.168.2.5	116.202.190.18

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2024 17:21:12.873646021 CEST	49712	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.873819113 CEST	49714	5432	192.168.2.5	116.202.190.18
Jun 7, 2024 17:21:12.878635883 CEST	5432	49714	116.202.190.18	192.168.2.5
Jun 7, 2024 17:21:13.718590021 CEST	5432	49714	116.202.190.18	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2024 17:21:04.512676954 CEST	58913	53	192.168.2.5	1.1.1.1
Jun 7, 2024 17:21:04.519785881 CEST	53	58913	1.1.1.1	192.168.2.5
Jun 7, 2024 17:21:25.621989965 CEST	53	49795	1.1.1.1	192.168.2.5
Jun 7, 2024 17:21:40.356259108 CEST	53	55550	162.159.36.2	192.168.2.5
Jun 7, 2024 17:21:40.977365971 CEST	49906	53	192.168.2.5	1.1.1.1
Jun 7, 2024 17:21:40.985791922 CEST	53	49906	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 7, 2024 17:21:04.512676954 CEST	192.168.2.5	1.1.1.1	0x9fe0	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
Jun 7, 2024 17:21:40.977365971 CEST	192.168.2.5	1.1.1.1	0xb45f	Standard query (0)	198.187.3.20.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 7, 2024 17:21:04.519785881 CEST	1.1.1.1	192.168.2.5	0x9fe0	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
Jun 7, 2024 17:21:40.985791922 CEST	1.1.1.1	192.168.2.5	0xb45f	Name error (3)	198.187.3.20.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false

HTTP Request Dependency Graph

- t.me

Statistics

Behavior

System Behavior

Analysis Process: file.exe PID: 6360, Parent PID: 1028

General

Target ID:	0
Start time:	11:21:02
Start date:	07/06/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0xff0000
File size:	442'408 bytes
MD5 hash:	7DC8189F70CC34E18EA7AF8FDEAC4142
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: 00000000.00000002.2070870185.0000000001023000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

Analysis Process: RegAsm.exe PID: 2780, Parent PID: 6360

General

Target ID:	2
Start time:	11:21:03
Start date:	07/06/2024
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:	0xa90000
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: 00000002.00000002.3325415366.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000002.00000002.3325415366.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	high
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGHJJEHDHCA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	417FAB	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\ProgramData\ECGHJJEHDHCA\DBKKFC	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	4073EE	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\BGDGHJ	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	40DE5F	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGHJJEHDHCA\HJJKFB	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	40D004	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\FBKECF	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	40DBC6	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\EBGDHJ	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	4073EE	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\BFCGDA	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	40DE5F	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\IDAEHC	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	40D004	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\JEHIID	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	40DBC6	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGHJJEHDHCA\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGHJJEHDHCA\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGHJJEHDHCA\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGHJJEHDHCA\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGHJJEHDHCA\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGHJJEHDHCA\DBKKFC	success or wait	1	407905	DeleteFileA
C:\ProgramData\ECGHJJEHDHCA\BGDGHJ	success or wait	1	40DF55	DeleteFileA
C:\ProgramData\ECGHJJEHDHCA\HJJKFB	success or wait	1	40D2A2	DeleteFileA
C:\ProgramData\ECGHJJEHDHCA\FBKECF	success or wait	1	40DD46	DeleteFileA
C:\ProgramData\ECGHJJEHDHCA\EBGDHJ	success or wait	1	407905	DeleteFileA
C:\ProgramData\ECGHJJEHDHCA\BFCGDA	success or wait	1	40DF55	DeleteFileA
C:\ProgramData\ECGHJJEHDHCA\IDAEHC	success or wait	1	40D2A2	DeleteFileA
C:\ProgramData\ECGHJJEHDHCA\JEHIID	success or wait	1	40DD46	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9C680Q69\sqls[1].dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1e fd 37 fd 5a fd 59 fd 5a fd 59 fd 5a fd 59 fd 11 fd 5a fd 6e fd 59 fd 11 fd 5c fd f3 59 fd 11 fd 5d fd 7f fd 59 fd 11 fd 58 fd 59 fd 59 fd 5a fd 58 fd 33 59 fd 4f fd 5c fd 45 fd 59 fd 4f fd 5d fd 55 fd 59 fd 4f fd 5a fd 4c fd 59 fd 6c 33 5d fd 5b fd 59 fd 6c 33 59 fd 5b fd 59 fd 6c 33 fd fd 5b fd 59 fd 6c 33 5b fd 5b fd 59 fd 52 69 63 68 5a fd 59 fd 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7ZYZYZYZnY\Y]Y XYYZXYO\EYO]UYOZLYl3][Yl3Y[Yl3[Yl3[[YRichZY	success or wait	2265	40433D	InternetReadFile
C:\ProgramData\ECGHJJEHDHCA\DBKKFC	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	4073EE	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGHJJEHDHCA\BGDGHJ	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	40DE5F	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\HJJKFB	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	40D004	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGHJJEHDHCA\FBKECF	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	SQLite format 3@ 4!.j1	success or wait	1	40DBC6	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\EBGDHJ	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 6a fd 0d 0d 24 00 04 0a 0c 00 0f 67 0f fd 0a 0c 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j$g	success or wait	1	4073EE	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGHJJEHDHCA\BFCGDA	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 26 00 00 00 00 00 00 00 00 00 00 00 1f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ &.j	success or wait	2	40DE5F	CopyFileA
C:\ProgramData\ECGHJJEHDHCA\IDAEHC	0	51200	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 02 07 fd 00 00 00 00 18 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	40D004	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGHJJEHDHCA\JEHIID	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 36 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y6.jW	success or wait	2	40DBC6	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	601365	success or wait	1	406D43	ReadFile
C:\ProgramData\ECGHJJEHDHCA\DBKKFC	0	100	success or wait	4	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\BGDGHJ	0	100	success or wait	12	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\HJJKFB	0	100	success or wait	6	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\FBKECF	0	100	success or wait	9	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\FBKECF	0	100	success or wait	9	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\FBKECF	0	100	success or wait	9	1B68FE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	44137	success or wait	1	406D43	ReadFile
C:\ProgramData\ECGHJJEHDHCA\EBGDHJ	0	100	success or wait	16	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\IDAEHC	0	100	success or wait	7	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\JEHIID	0	100	success or wait	13	1B68FE09	ReadFile
C:\ProgramData\ECGHJJEHDHCA\JEHIID	0	100	success or wait	13	1B68FE09	ReadFile

Disassembly

⊘ **No disassembly**