ID: 1454088
Sample Name: f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe
Cookbook: default.jbs
Time: 20:21:05
Date: 08/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

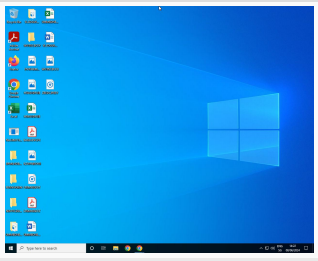
Windows Analysis Report

f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe

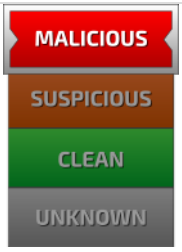
Overview

General Information

Sample name:	f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe
Analysis ID:	1454088
MD5:	9c2b900d014b…
SHA1:	e5705841f68d9..
SHA256:	f9e3368715092..
Tags:	exe Stealc
Infos:	



Detection



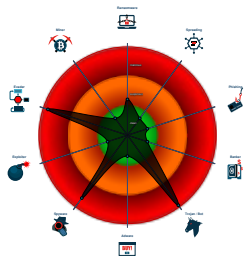
Mars Stealer, Stealc, Vidar

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Yara detected AntiVM3
- Yara detected Mars stealer
- Yara detected Stealc
- Yara detected Vidar stealer
- AI detected suspicious sample

Classification



Process Tree

- **System is w10x64**
- f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe (PID: 7520 cmdline: "C:\Users\user\Desktop\f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe" MD5: 9C2B900D014BA5B9DFD0CA6CEF201753)
  - conhost.exe (PID: 7528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - aspnet_regiis.exe (PID: 7596 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe" MD5: 5D1D74198D75640E889F0A577BBF31FC)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Stealc	Stealc is an information stealer advertised by its presumed developer Plymouth on Russian-speaking underground forums and sold as a Malware-as-a-Service since January 9, 2023. According to Plymouth's statement, stealc is a non-resident stealer with flexible data collection settings and its development is relied on other prominent stealers: Vidar, Raccoon, Mars and Redline.Stealc is written in C and uses WinAPI functions. It mainly targets date from web browsers, extensions and Desktop application of cryptocurrency wallets, and from other applications (messengers, email clients, etc.). The malware downloads 7 legitimate third-party DLLs to collect sensitive data from web browsers, including sqlite3.dll, nss3.dll, vcruntime140.dll, mozglue.dll, freebl3.dll, softokn3.dll and msvcp140.dll. It then exfiltrates the collected information file by file to its C2 server using HTTP POST requests.	No Attribution	http://https://any.run/cybersecurity-blog/crackedcantil-breakdown/https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-2/https://cocomelonc.github.io/book/2023/12/13/malwild-book.htmlhttps://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-stealc-cbe5c94b84af	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.stealc

Name	Description	Attribution	Blogpost URLs	Link

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: StealC


```
{
  "C2 url": "http://23.88.106.134/6a9f8e2503d99c04.php"
}
```


Threatname: Vidar


```
{
  "C2 url": "http://23.88.106.134/6a9f8e2503d99c04.php"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Stealc_1	Yara detected Stealc	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1699865852.000000006CC3D000.00000004.00000001.01000000.00000007.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000002.1699865852.000000006CC3D000.00000004.00000001.01000000.00000007.sdmp	JoeSecurity_MarsStealer	Yara detected Mars stealer	Joe Security	
00000002.00000002.1806482282.0000000002BA7000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Stealc	Yara detected Stealc	Joe Security	
00000002.00000002.1805843043.0000000002750000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000002.00000002.1805843043.0000000002750000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_MarsStealer	Yara detected Mars stealer	Joe Security	

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.aspnet_regiis.exe.2750000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.aspnet_regiis.exe.2750000.0.raw.unpack	JoeSecurity_MarsStealer	Yara detected Mars stealer	Joe Security	
0.2.f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe.6cc3d000.5.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe.6cc3d000.5.unpack	JoeSecurity_MarsStealer	Yara detected Mars stealer	Joe Security	

Source	Rule	Description	Author	Strings
2.2.aspnet_regiis.exe.2750000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/Stealc Active C2 Responding with browsers Config M1 - Source IP: 23.88.106.134 - Destination IP: 192.168.2.4

Timestamp:	06/08/24-20:21:59.805841
SID:	2051828
Source Port:	80
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Stealc Requesting browsers Config from C2 - Source IP: 192.168.2.4 - Destination IP: 23.88.106.134

Timestamp:	06/08/24-20:21:59.555146
SID:	2044244
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Stealc/Vidar Stealer Active C2 Responding with plugins Config M1 - Source IP: 23.88.106.134 - Destination IP: 192.168.2.4

Timestamp:	06/08/24-20:22:00.160152
SID:	2051831
Source Port:	80
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [SEKOIA.IO] Win32/Stealc C2 Check-in - Source IP: 192.168.2.4 - Destination IP: 23.88.106.134

Timestamp:	06/08/24-20:21:58.692257
SID:	2044243
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Stealc Requesting plugins Config from C2 - Source IP: 192.168.2.4 - Destination IP: 23.88.106.134

Timestamp:	06/08/24-20:21:59.902142
SID:	2044246
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- AI detected suspicious sample
- Machine Learning detection for dropped file
- Machine Learning detection for sample
- Sample uses string decryption to hide its real strings

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

System Summary

- PE file contains section with special chars
- PE file has nameless sections

Data Obfuscation

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion

- Yara detected AntiVM3
- Found evasive API chain (may stop execution after checking locale)

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 Mars stealer
- Yara detected Stealc
- Yara detected Vidar stealer
- Found many strings related to Crypto-Wallets (likely being stolen)
- Tries to harvest and steal Bitcoin Wallet information
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Crypto Currency Wallets
- Tries to steal Mail credentials (via file / registry access)

Remote Access Functionality

Yara detected Mars stealer

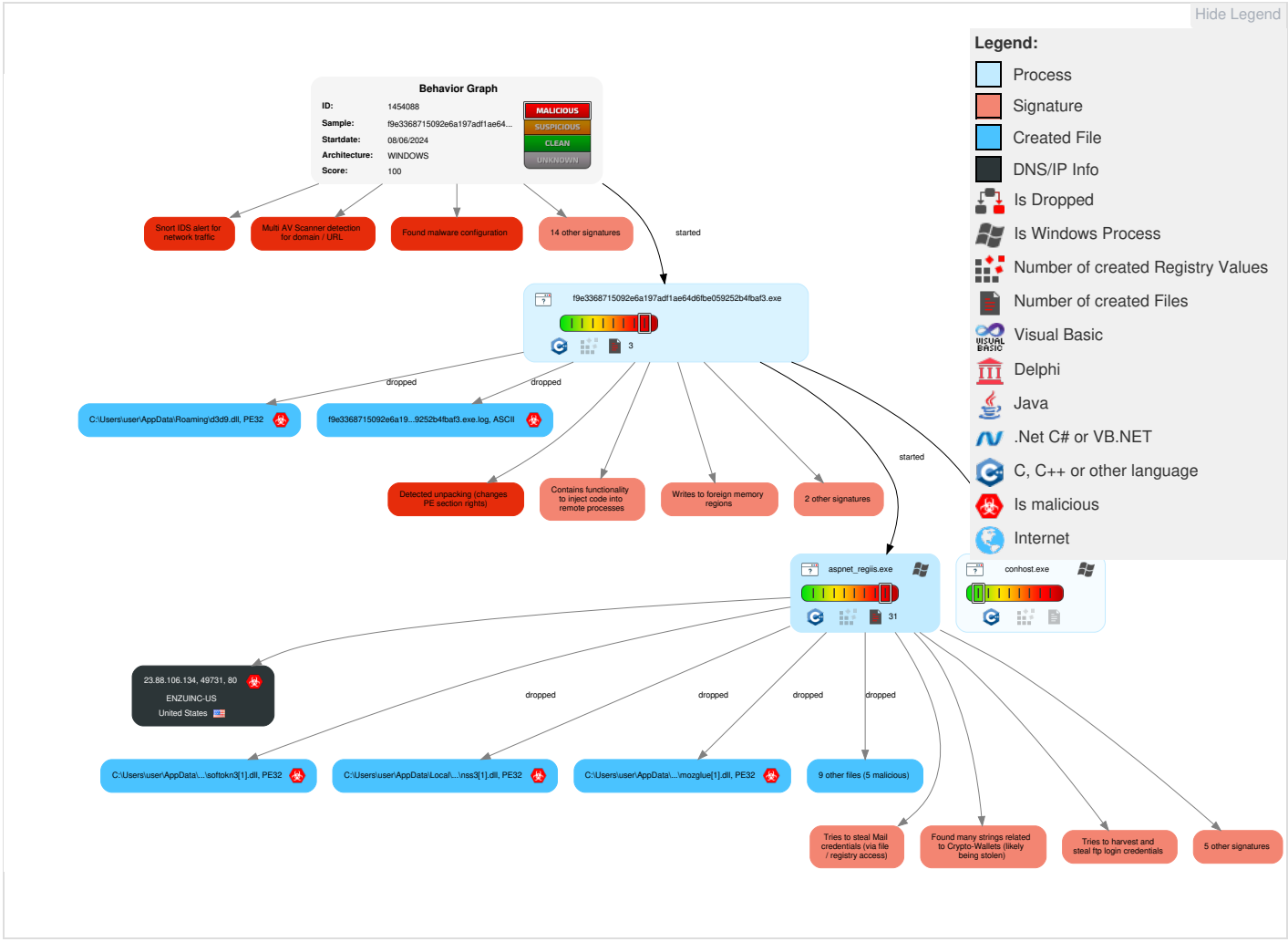
Yara detected Stealc

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 1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	1 2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	5 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	4 Data from Local System	2 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	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	2 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 2 Software Packing	NTDS	1 4 4 System Information Discovery	Distributed Component Object Model	1 Email Collection	1 1 2 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 2 1 Security Software Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Masquerading	Cached Domain Credentials	1 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	1 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
f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe	38%	ReversingLabs	Win32.Trojan.Amadey	
f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe	35%	Virustotal		Browse
f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\d3d9.dll	100%	Joe Sandbox ML		
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\freebl3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\mozglue[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\msvcp140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\nss3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\softokn3[1].dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\vcruntime140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\d3d9.dll	79%	ReversingLabs	Win32.Trojan.LummaStealer	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	URL Reputation	safe	
http://23.88.106.134/6a9f8e2503d99c04.phpGS	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phpwser	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/softokn3.dllOV	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://23.88.106	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Virustotal		Browse
http://23.88.106.134/6a9f8e2503d99c04.php	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phpC	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Virustotal		Browse
http://23.88.106.134/6a9f8e2503d99c04.php?S	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.php	13%	Virustotal		Browse
http://23.88.106.134/566d6e1ec8db6394/nss3.dllj9	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phpm	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/nss3.dllpera	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phpiSS	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/sqlite3.dll	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phppenSSH	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/mozglue.dllAV	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/msvcp140.dll	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phpz	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17chost.exe	0%	Avira URL Cloud	safe	
http://23.88.106.134/566d6e1ec8db6394/msvcp140.dll	12%	Virustotal		Browse
http://23.88.106.134/6a9f8e2503d99c04.php513e43049a24c4f8a56ff24fb86a0b	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016.exe	0%	Avira URL Cloud	safe	
http://23.88.106.134/6a9f8e2503d99c04.phpition:	100%	Avira URL Cloud	malware	
http://www.sqlite.org/copyright.html.	0%	Avira URL Cloud	safe	
http://23.88.106.134y	0%	Avira URL Cloud	safe	
http://www.mozilla.com/en-US/blocklist/	0%	Avira URL Cloud	safe	
http://https://mozilla.org0/	0%	Avira URL Cloud	safe	
http://www.sqlite.org/copyright.html.	0%	Virustotal		Browse
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://www.mozilla.com/en-US/blocklist/	0%	Virustotal		Browse
http://23.88.106.134/566d6e1ec8db6394/sqlite3.dll	13%	Virustotal		Browse
http://23.88.106.134/6a9f8e2503d99c04.phpdus.wallet	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://23.88.106.134/566d6e1ec8db6394/softokn3.dll	100%	Avira URL Cloud	malware	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	0%	Avira URL Cloud	safe	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	0%	Virustotal		Browse
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Virustotal		Browse
http://https://www.ecosia.org/newtab/	0%	Virustotal		Browse
http://https://www.ecosia.org/newtab/	0%	Avira URL Cloud	safe	
http://23.88.106.134/566d6e1ec8db6394/mozglue.dll	12%	Virustotal		Browse
http://23.88.106.134/566d6e1ec8db6394/mozglue.dll	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/freebl3.dllYW	100%	Avira URL Cloud	malware	
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	0%	Avira URL Cloud	safe	
http://23.88.106.134/566d6e1ec8db6394/softokn3.dll	12%	Virustotal		Browse
http://23.88.106.134/6a9f8e2503d99c04.php)	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phpcS	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/freebl3.dlleV	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/freebl3.dll	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/vcruntime140.dll3x	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.phpition:	12%	Virustotal		Browse
http://23.88.106.134	100%	Avira URL Cloud	malware	
http://23.88.106.134/566d6e1ec8db6394/nss3.dll	100%	Avira URL Cloud	malware	
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	0%	Virustotal		Browse
http://23.88.106.134/566d6e1ec8db6394/vcruntime140.dll4	100%	Avira URL Cloud	malware	
http://https://support.mozilla.org	0%	Avira URL Cloud	safe	
http://23.88.106.134/566d6e1ec8db6394/vcruntime140.dll	100%	Avira URL Cloud	malware	
http://23.88.106.134/6a9f8e2503d99c04.php6	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://23.88.106.134/6a9f8e2503d99c04.php	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/sqlite3.dll	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/msvcp140.dll	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/softokn3.dll	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/mozglue.dll	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/freebl3.dll	true	• Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/nss3.dll	true	• Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/vcruntime140.dll	true	• Avira URL Cloud: malware	unknown

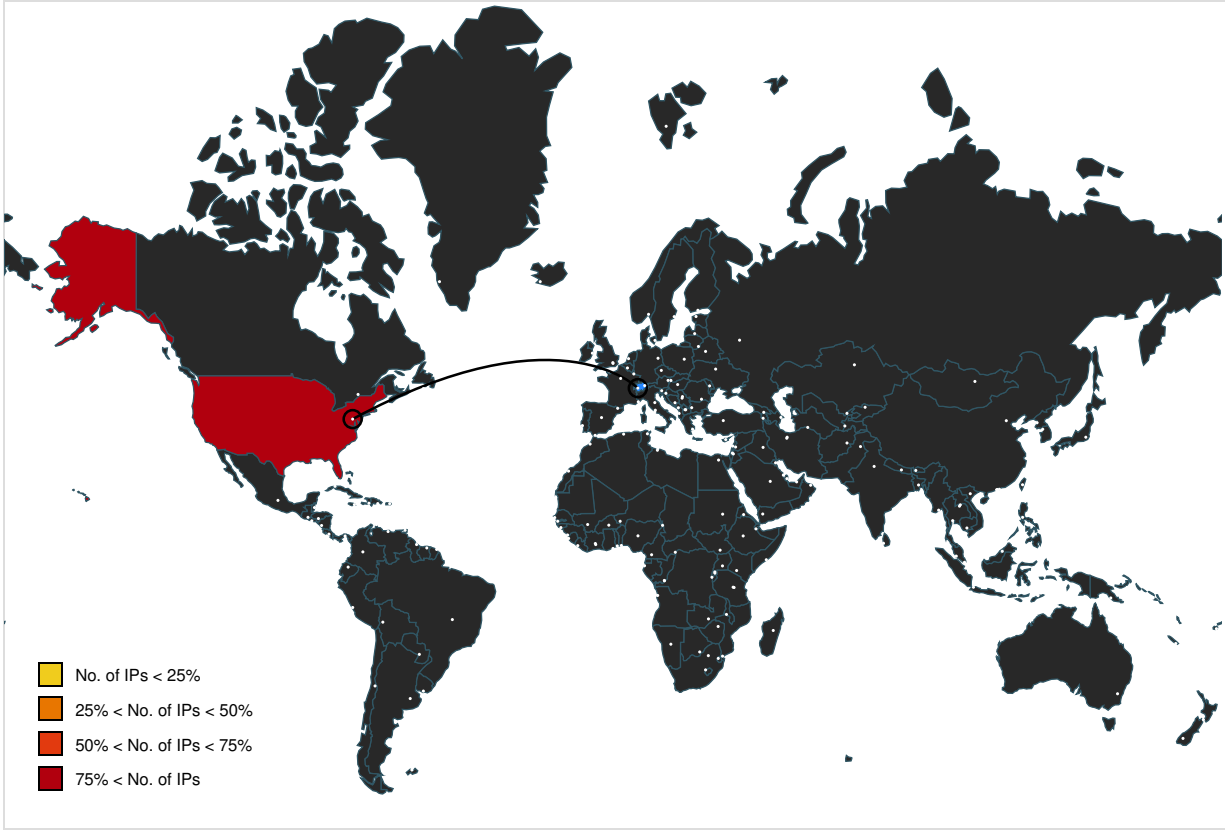
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://23.88.106.134/6a9f8e2503d99c04.phpGS	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpwser	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002C03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/chrome_newtab	aspnet_regiis.exe, 00000002.00000003.1729693945.0000000002C58000.00000004.00000020.00020000.00000000.sdmp, KJJJDHI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.zvXrErQ5GYDF	ECAKKKKJDBKKFIEBKEHDGCAFCB.2.dr	false	• Avira URL Cloud: safe	unknown
http://23.88.106.134/566d6e1ec8db6394/softokn3.dllOV	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BEA000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	aspnet_regiis.exe, 00000002.00000003.172 9693945.0000000002C58000.00000004.000000 20.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://23.88.106	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002C03000.00000004.000000 20.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpC	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BEA000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	aspnet_regiis.exe, 00000002.00000003.172 9693945.0000000002C58000.00000004.000000 20.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	aspnet_regiis.exe, 00000002.00000003.172 6461054.0000000022DDD000.00000004.000000 20.00020000.00000000.sdmp, aspnet_regiis.exe, 00000002.00000002.1805898041.000000000279B00 0.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.php?S	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BEA000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/nss3.dllj9	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BD7000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpm	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002C03000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/nss3.dllpera	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BEA000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpiSS	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BEA000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/6a9f8e2503d99c04.phppenSSH	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002C03000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	aspnet_regiis.exe, 00000002.00000003.172 9693945.0000000002C58000.00000004.000000 20.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• URL Reputation: safe	unknown
http://23.88.106.134/566d6e1ec8db6394/mozglue.dllAV	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BEA000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpz	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002C03000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17chost.exe	aspnet_regiis.exe, 00000002.00000002.180 5898041.000000000279B000.00000040.000004 00.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.php513e43049a24c4f8a56ff24fb86a0b	aspnet_regiis.exe, 00000002.00000002.180 5898041.000000000279B000.00000040.000004 00.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016.exe	aspnet_regiis.exe, 00000002.00000002.180 5898041.000000000279B000.00000040.000004 00.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpition:	aspnet_regiis.exe, 00000002.00000002.180 5898041.000000000279B000.00000040.000004 00.00020000.00000000.sdmp	false	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.sqlite.org/copyright.html.	aspnet_regiis.exe, 00000002.00000002.181 7001659.000000001CE4E000.00000004.000000 20.00020000.00000000.sdmp, aspnet_regiis.exe, 00000002.00000002.1824142050.0000000061ED300 0.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://23.88.106.134y	aspnet_regiis.exe, 00000002.00000002.180 6482282.0000000002BA7000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mozilla.com/en-US/blocklist/	aspnet_regiis.exe, aspnet_regiis.exe, 00000002.000 00002.1824348994.000000006C31D000.000000 02.00000001.01000000.0000000B.sdmp, mozglue[1].dll.2.dr, mozglue.dll.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://mozilla.org0/	freebl3.dll.2.dr, nss3[1].dll.2.dr, softokn3[1].dll.2.dr, softokn3.dll.2.dr, mozglue[1].dll.2.dr, mozglue.dll.2.dr, nss3.dll.2.dr, freebl3[1].dll.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	aspnet_regiis.exe, 00000002.00000003.1729693945.0000000002C58000.00000004.00000020.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpdus.wallet	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002C03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	aspnet_regiis.exe, 00000002.00000003.1729693945.0000000002C58000.00000004.00000020.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	aspnet_regiis.exe, 00000002.00000003.1726461054.0000000022DDD000.00000004.00000020.00020000.00000000.sdmp, aspnet_regiis.exe, 00000002.00000002.1805898041.000000000279B000.00000040.00000400.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	aspnet_regiis.exe, 00000002.00000003.1729693945.0000000002C58000.00000004.00000020.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://23.88.106.134/566d6e1ec8db6394/freebl3.dllYW	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	ECAKKKKJDBKKFIEBKEHDGCAFCB.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.php)	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002C03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ac.ecosia.org/autocomplete?q=	aspnet_regiis.exe, 00000002.00000003.1729693945.0000000002C58000.00000004.00000020.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• URL Reputation: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.phpcS	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/freebl3.dlleV	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/vcruntime140.dll3x	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://23.88.106.134	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002BA7000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://23.88.106.134/566d6e1ec8db6394/vcruntime140.dll4	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002C03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://support.mozilla.org	ECAKKKKJDBKKFIEBKEHDGCAFCB.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	aspnet_regiis.exe, 00000002.00000003.1729693945.0000000002C58000.00000004.00000020.00020000.00000000.sdmp, KJJJJDHI.2.dr	false	• URL Reputation: safe	unknown
http://23.88.106.134/6a9f8e2503d99c04.php6	aspnet_regiis.exe, 00000002.00000002.1806482282.0000000002C03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.88.106.134	unknown	United States		18978	ENZUINC-US	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1454088
Start date and time:	2024-06-08 20:21:05 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 7m 17s
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:	f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@4/23@0/1
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SIHClient.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, dns.msftncsi.com, fe3cr.delivery.mp.microsoft.com
- HTTP raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

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\AFIIEBGCAAECBGCBGCBK

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j..... ....

C:\ProgramData\AFIIEBGCAAECBGCBGCBKEHIJEB

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.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:/xGZR8wbtxq5uWRHKloIN7YItnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621C3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\ProgramData\BFHJECAA

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.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:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\ProgramData\ECAKKKKJDBKKFIEBKEHD

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.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:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4574
Malicious:	false

Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....O}.....

C:\ProgramData\ECAKKKKJDBKKFIEBKEHDGCAFCB

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.037963276276857943
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWZWdgokBQNba9D3DO/JxW/QHI:58r54w0VW3xWZWdOBQFal3dQ
MD5:	C0FDF21AE11A6D1FA1201D502614B622
SHA1:	11724034A1CC915B061316A96E79E9DA6A00ADE8
SHA-256:	FD4EB46C81D27A9B3669C0D249DF5CE2B49E5F37B42F917CA38AB8831121ADAC
SHA-512:	A6147C196B033725018C7F28C1E75E20C2113A0C6D8172F5EABCB8FF334EA6CE10B758FFD1D22D50B4DB5A0A21BCC15294AC44E94D973F7A3EB9F8558F3176 B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>..

C:\ProgramData\JEHIDHDAKJDHJKEBFIEHCAAEHD

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153
Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE3617890459
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....}..}.....

C:\ProgramData\KJJJJDHI

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

C:\ProgramData\freebl3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	685392
Entropy (8bit):	6.872871740790978
Encrypted:	false
SSDEEP:	12288:4gPbPpxMofhPNN0+RXBrp3M5pzRN4l2SQ+PEu9tUs/abAQb51FW/IzkOfWPO9UN7:4gPbPp9NNP0BgInfW2WMC4M+hW
MD5:	550686C0EE48C386DFCB40199BD076AC
SHA1:	EE5134DA4D3EFCB466081FB6197BE5E12A5B22AB
SHA-256:	EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
SHA-512:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....4.....p.....@A....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F..0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..."..... .....@..B.....

C:\ProgramData\mozglue.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.833616094889818
Encrypted:	false
SSDEEP:	12288:BlSyAom/gcRKMdRm4wFkRHuyG4RRGJVDjMk/x21R8gY/r:BKgcRKMdRm4wFkVVDGJVv//x21R8br
MD5:	C8FD9BE83BC728CC04BEFFAFC2907FE9
SHA1:	95AB9F701E0024CEDFBD312BCFE4E726744C4F2E
SHA-256:	BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
SHA-512:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B40
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....^.....j.....@A....`...W.....P/...0...A...S.....h.....Z.....text...a..... ..`.rdata.....@..@.data...D.....@....00cfg.....@..@.tls.....@....rsrc..... .....@..@.reloc...A...0...B.....@..B.....

C:\ProgramData\msvcp140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	450024
Entropy (8bit):	6.673992339875127
Encrypted:	false
SSDEEP:	12288:McPa9C9VbL+3Omy5CvyOvzeOKdqhUgiW6QR7t5s03Ooc8dHkC2esGAWf:McPa90Vbky5CvyUeOKn03Ooc8dHkC2eN
MD5:	5FF1FCA37C466D6723EC67BE93B51442
SHA1:	34CC4E158092083B13D67D6D2BC9E57B798A303B
SHA-256:	5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
SHA-512:	4802EF62630C521D83A1D333969593FB00C9B38F82B4D07F70FBD21F495FEA9B3F67676064573D2C71C42BC6F701992989742213501B16087BB6110E337C7546
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._..._..._)n..._....._...^.".._..^..._..\..._..[..._..Z..._..._..._.....]..._.Rich.._.....PE..L.....0].....!....(.....`.....@.....,....@A.....g.....r.....A.....=..`x..8.....w..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc.....Z.....@..@.reloc...=.....>..^.....@..B.....

C:\ProgramData\nss3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2046288
Entropy (8bit):	6.787733948558952
Encrypted:	false
SSDEEP:	49152:fECf12gikHlnKGxJRIB+y5nvxnaOSJ3HFNWYrVvE4CQsgzMmQfTU1NrWmy4KoAzh:J7Tf8J1Q+SS5/nr
MD5:	1CC453CDF74F31E4D913FF9C10ACDDE2
SHA1:	6E85EAE544D6E965F15FA5C39700FA7202F3AAFE
SHA-256:	AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5
SHA-512:	DD9FF4E06B00DC831439BAB11C10E9B2AE864EA6E780D3835EA7468818F35439F352EF137DA111EFCDF2BB6465F6CA486719451BF6CF32C6A4420A56B1D6457 1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....`.....p.....l- ...@A.... .....&.....@....P..x.....P/...`..\.....\....&..@.....text..... ..`.rdata..l.....@..@.data...DR.. .....@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\...`.....@..B..... ....

C:\ProgramData\softokn3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	257872
Entropy (8bit):	6.727482641240852
Encrypted:	false
SSDEEP:	6144:/yF/zX2zfRkU62THVh/T2AhZxv6A31obD6Hq/8jis+FvtVRpsAAs0o8OqTYz+xnU:/yRzX2zfRkX2T1h/SA5PF9m8jJqKYz+y
MD5:	4E52D739C324DB8225BD9AB2695F262F
SHA1:	71C3DA43DC5A0D2A1941E874A6D015A071783889
SHA-256:	74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
SHA-512:	2D4168A69082A9192B9248F7331BD806C260478FF817567DF54F997D7C3C7D640776131355401E4BDB9744E246C36D658CB24B18DE67D8F23F10066E5FE445F6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....P.....Sg ....@A.....Dv..S....w.....P/.....5..8q.....{.....text...&..... ..`.rdata.....@..@.da ta.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... ....

C:\ProgramData\vcruntime140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80880
Entropy (8bit):	6.920480786566406
Encrypted:	false
SSDEEP:	1536:lw2886xv555et/MCsjw0BuRK3jteo3ecbA2W86b+Ld:lw28V55At/zqw+lq9ecbA2W8H
MD5:	A37EE36B536409056A86F50E67777DD7
SHA1:	1CAFA159292AA736FC595FC04E16325B27CD6750
SHA-256:	8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825
SHA-512:	3A7C260646315CF8C01F44B2EC60974017496BD0D80DD055C7E43B707CADBA2D63AAB5E0EFD435670AA77886ED86368390D42C4017FC433C3C4B9D1C47D0F3 6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L...|.0]....."!.....0.....m....@A.....A... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe.log

Process:	C:\Users\user\Desktop\f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.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:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\freebl3[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	685392
Entropy (8bit):	6.872871740790978
Encrypted:	false
SSDEEP:	12288:4gPbPpxMofhPNN0+RXBrp3M5pzRN4l2SQ+PEu9tUs/abAQb51FW/IzkOfWPO9UN7:4gPbPp9NNP0BgInfW2WMC4M+hW
MD5:	550686C0EE48C386DFCB40199BD076AC
SHA1:	EE5134DA4D3EFCB466081FB6197BE5E12A5B22AB
SHA-256:	EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
SHA-512:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....4.....p.....@A....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F..0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..".....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\mozglue[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.833616094889818
Encrypted:	false
SSDEEP:	12288:BlSyAom/gcRKMdRm4wFkRHuyG4RRGJVDjMk/x21R8gY/r:BKgcRKMdRm4wFkVVDGJVv//x21R8br
MD5:	C8FD9BE83BC728CC04BEFFAFC2907FE9
SHA1:	95AB9F701E0024CEDFBD312BCFE4E726744C4F2E
SHA-256:	BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
SHA-512:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B40
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....^.....j.....@A....`...W.....P/...0...A...S.....h.....Z.....text...a..... ..`.rdata.....@..@.data...D.....@....00cfg.....@..@.tls.....@....rsrc..... .....@..@.reloc...A...0...B.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\msvcp140[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	450024
Entropy (8bit):	6.673992339875127
Encrypted:	false
SSDEEP:	12288:McPa9C9VbL+3Omy5CvyOvzeOKdqhUgiW6QR7t5s03Ooc8dHkC2esGAWf:McPa90Vbky5CvyUeOKn03Ooc8dHkC2eN
MD5:	5FF1FCA37C466D6723EC67BE93B51442
SHA1:	34CC4E158092083B13D67D6D2BC9E57B798A303B
SHA-256:	5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
SHA-512:	4802EF62630C521D83A1D333969593FB00C9B38F82B4D07F70FBD21F495FEA9B3F67676064573D2C71C42BC6F701992989742213501B16087BB6110E337C7546
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._..._..._.)n...._....._...^."._..^..._..\..._..[..._..Z..._..._..._......_..]..._.Rich.._.....PE..L.....0]......"!.....(.....`.....@.....,....@A.....g.....r.....A.....=..`x..8.....w..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc.....Z.....@..@.reloc...=.....>...^.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\nss3[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2046288
Entropy (8bit):	6.787733948558952
Encrypted:	false
SSDEEP:	49152:fECf12gikHlnKGxJRIB+y5nvxnaOSJ3HFNWYrVvE4CQsgzMmQfTU1NrWmy4KoAzh:J7Tf8J1Q+SS5/nr
MD5:	1CC453CDF74F31E4D913FF9C10ACDDE2
SHA1:	6E85EAE544D6E965F15FA5C39700FA7202F3AAFE
SHA-256:	AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5
SHA-512:	DD9FF4E06B00DC831439BAB11C10E9B2AE864EA6E780D3835EA7468818F35439F352EF137DA111EFCDF2BB6465F6CA486719451BF6CF32C6A4420A56B1D64571
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....`.....p.....l- ...@A.....&.....@....P..x.....P/...`..\.....\....&..@.....text..... ..`.rdata..l.....@..@.data...DR.....@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\...`.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\softokn3[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	257872
Entropy (8bit):	6.727482641240852
Encrypted:	false
SSDEEP:	6144:/yF/zX2zfRkU62THVh/T2AhZxv6A31obD6Hq/8jis+FvtVRpsAAs0o8OqTYz+xnU:/yRzX2zfRkX2T1h/SA5PF9m8jJqKYz+y
MD5:	4E52D739C324DB8225BD9AB2695F262F
SHA1:	71C3DA43DC5A0D2A1941E874A6D015A071783889
SHA-256:	74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
SHA-512:	2D4168A69082A9192B9248F7331BD806C260478FF817567DF54F997D7C3C7D640776131355401E4BDB9744E246C36D658CB24B18DE67D8F23F10066E5FE445F6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....P.....Sg....@A.....Dv..S....w.....P/.....5..8q.....{.....text...&..... ..`.rdata.....@..@.data.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\vcruntime140[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80880

Entropy (8bit):	6.920480786566406
Encrypted:	false
SSDEEP:	1536:lw2886xv555et/MCsjw0BuRK3jteo3ecbA2W86b+Ld:lw28V55At/zqw+lq9ecbA2W8H
MD5:	A37EE36B536409056A86F50E67777DD7
SHA1:	1CAFA159292AA736FC595FC04E16325B27CD6750
SHA-256:	8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825
SHA-512:	3A7C260646315CF8C01F44B2EC60974017496BD0D80DD055C7E43B707CADBA2D63AAB5E0EFD435670AA77886ED86368390D42C4017FC433C3C4B9D1C47D0F36
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L...|.0]....."!.....0.....m....@A.....A... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\cookies.sqlite-shm

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.017262956703125623
Encrypted:	false
SSDEEP:	3:G8lQs2TSlElQs2TtPRp//:G0QjSaQjrpX
MD5:	B7C14EC6110FA820CA6B65F5AEC85911
SHA1:	608EEB7488042453C9CA40F7E1398FC1A270F3F4
SHA-256:	FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
SHA-512:	D8D75760F29B1E27AC9430BC4F4FFCEC39F1590BE5AEF2BFB5A535850302E067C288EF59CF3B2C5751009A22A6957733F9F80FA18F2B0D33D90C068A3F08F3B
Malicious:	false
Preview:	..-.....8...5.....-.....8...5..... ....

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\places.sqlite-shm

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.017262956703125623
Encrypted:	false
SSDEEP:	3:G8lQs2TSlElQs2TtPRp//:G0QjSaQjrpX
MD5:	B7C14EC6110FA820CA6B65F5AEC85911
SHA1:	608EEB7488042453C9CA40F7E1398FC1A270F3F4
SHA-256:	FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
SHA-512:	D8D75760F29B1E27AC9430BC4F4FFCEC39F1590BE5AEF2BFB5A535850302E067C288EF59CF3B2C5751009A22A6957733F9F80FA18F2B0D33D90C068A3F08F3B
Malicious:	false
Preview:	..-.....8...5.....-.....8...5..... ....

C:\Users\user\AppData\Roaming\d3d9.dll

Process:	C:\Users\user\Desktop\f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	272896
Entropy (8bit):	6.785813762497204
Encrypted:	false
SSDEEP:	6144:XYaqOCMQK9syh0bxdWPhT917U4ji8U7kV:oaqOCMRyx2/fjn
MD5:	A16BFDD7C9F753A43F3EAA5522BA9D9D
SHA1:	36381482314AB4845531E4875C1FE520B50D1FE4

SHA-256:	E0B2AA87DAFB8977C806C5BFADA424E7DAE2E41995B8974D72EE455513262EA5
SHA-512:	FC700EF5A63F3CA9141991F9AEA64F1B5958C6895C27B1763791736219C0CDD8D033B9D4D7F9A4D435AB86A14C5EC4A12F69298BD7A9EE6FADE9EE98EFB1B846
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.)...GQ..GQ..GQL.DP..GQL.BP..GQL.CP..GQL.FP..GQ z<Q ..GQ..FQe.GQ.=BP..GQ.=CP..GQ.=DP..GQ..GQ..GQj=GP..GQj=EP..GQRich..GQ.....PE..L.....bf.....!...&.N.....~.....`.....`.....@... .....T...T...<.....@..... .....`...@.....`..P.....text....M.....N..... ..`.rdata...c...`...d...R.....@..@.data...\i .....`.....@....reloc.....@.....@..B..... .....

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.415848356186701
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe
File size:	474'624 bytes
MD5:	9c2b900d014ba5b9dfd0ca6cef201753
SHA1:	e5705841f68d9443ba5efb553aa9f87556e403e5
SHA256:	f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf317fab7b3e90281b5d05
SHA512:	5f92c1cff9312b100feca38c4ad8aa82af351d9ca01c420ed44f154fe8c1e3c9027fcffcf9578748601bc29708e8df0969bd4cdc1732a819fb37006a769b13d4
SSDEEP:	12288:4seLUscjnY6sJnCWH4UbmCJbbdKofwk/TsyVhpceSvbCq66imuXd6cWD/pWc0GMX:47U17
TLSH:	3FA4A89D766076DFC85BD0729AA81DB8FB5078BB431F4243902716ADAE5C89BCF140F2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....bf.....j..... ....@.. .....@.....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x47c00a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6662E9C7 [Fri Jun 7 11:06:47 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

Entrypoint Preview

Instruction
jmp dword ptr [0047C000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x307fc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x78000	0x6d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x7c000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x30000	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
A7B&<U	0x2000	0x2c594	0x2c600	02cd036eb91bd81e0b36971c82bf1b45	False	0.9998899647887324	data	7.998974089724877	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.text	0x30000	0x46730	0x46800	ec30b4931571fd884bfe8bc644b5b4eb	False	0.3267848238031915	data	4.520642074921792	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x6d8	0x800	468273f60eaf63ae5528e7b5d667ae35	False	0.36279296875	data	3.7387498824008096	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7a000	0xc	0x200	e81a80c38992ec6b3b4d5dcfcfc5314a	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x7c000	0x10	0x200	7ca58d1a0a472541553b5df07f5e79fd	False	0.044921875	Applesoft BASIC program data, first line number 3	0.14263576814887827	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_VERSION	0x780a0	0x44c	data			0.4
RT_MANIFEST	0x784ec	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/08/24-20:21:59.805841	TCP	2051828	ET TROJAN Win32/Stealc Active C2 Responding with browsers Config M1	80	49731	23.88.106.134	192.168.2.4
06/08/24-20:21:59.555146	TCP	2044244	ET TROJAN Win32/Stealc Requesting browsers Config from C2	49731	80	192.168.2.4	23.88.106.134
06/08/24-20:22:00.160152	TCP	2051831	ET TROJAN Win32/Stealc/Vidar Stealer Active C2 Responding with plugins Config M1	80	49731	23.88.106.134	192.168.2.4
06/08/24-20:21:58.692257	TCP	2044243	ET TROJAN [SEKOIA.IO] Win32/Stealc C2 Check-in	49731	80	192.168.2.4	23.88.106.134
06/08/24-20:21:59.902142	TCP	2044246	ET TROJAN Win32/Stealc Requesting plugins Config from C2	49731	80	192.168.2.4	23.88.106.134

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2024 20:21:58.686938047 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:21:58.691910028 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:21:58.691996098 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:21:58.692256927 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:21:58.697139025 CEST	80	49731	23.88.106.134	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2024 20:21:59.553096056 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:21:59.553186893 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:21:59.555145979 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:21:59.561285019 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:21:59.805840969 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:21:59.805902958 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:21:59.806415081 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:21:59.902142048 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:21:59.912898064 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.160151958 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.160202980 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.160242081 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.160276890 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.160315990 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.160330057 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.160387993 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.160387993 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.160410881 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.211610079 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.211685896 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.220216990 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.220278025 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.220308065 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.220340967 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.224417925 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.224447012 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.228542089 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.496449947 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.496597052 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.740082979 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.749938011 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995032072 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995050907 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995066881 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995081902 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995100021 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995114088 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995323896 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.995325089 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.995374918 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995392084 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995408058 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995444059 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.995460987 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995470047 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.995480061 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995490074 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995628119 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995642900 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:00.995645046 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:00.995704889 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118257046 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118359089 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118387938 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118426085 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118443012 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118459940 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118495941 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118521929 CEST	49731	80	192.168.2.4	23.88.106.134

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2024 20:22:01.118522882 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118549109 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118561029 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118602037 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118602991 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118638992 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118671894 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.118714094 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118714094 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.118833065 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.119492054 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.119525909 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.119563103 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.119563103 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.119586945 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.119596958 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.119618893 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.119637966 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.119663954 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.119712114 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.120668888 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.120703936 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.120739937 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.120748997 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.120771885 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.120779991 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.120795012 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.120815992 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.120855093 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.120884895 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.121778011 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.121855974 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.121931076 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.121964931 CEST	80	49731	23.88.106.134	192.168.2.4
Jun 8, 2024 20:22:01.121995926 CEST	49731	80	192.168.2.4	23.88.106.134
Jun 8, 2024 20:22:01.122000933 CEST	80	49731	23.88.106.134	192.168.2.4

UDP Packets

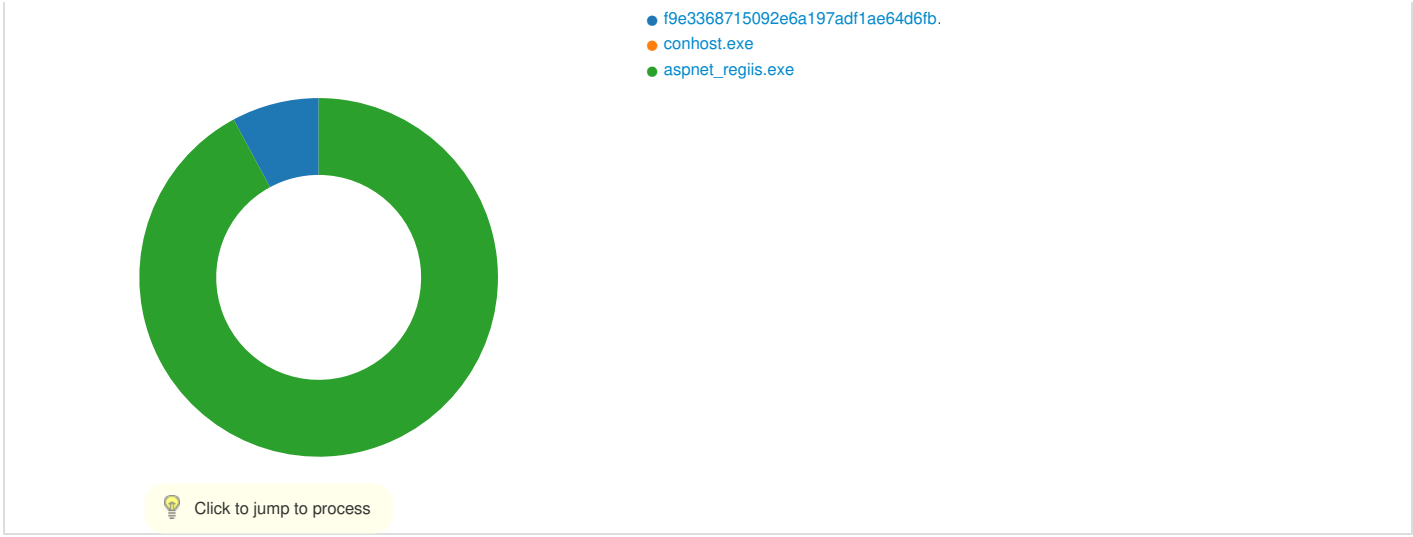
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 8, 2024 20:22:19.646400928 CEST	53	65147	1.1.1.1	192.168.2.4

HTTP Request Dependency Graph

- 23.88.106.134

Statistics

Behavior



System Behavior

Analysis Process: f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe PID: 7520, Parent PID: 2580

General

Target ID:	0
Start time:	14:21:57
Start date:	08/06/2024
Path:	C:\Users\user\Desktop\f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\f9e3368715092e6a197adf1ae64d6fbe059252b4fbaf3.exe"
Imagebase:	0x750000
File size:	474'624 bytes
MD5 hash:	9C2B900D014BA5B9DFD0CA6CEF201753
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: 00000000.00000002.1699865852.000000006CC3D000.00000004.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_MarsStealer, Description: Yara detected Mars stealer, Source: 00000000.00000002.1699865852.000000006CC3D000.00000004.00000001.01000000.00000007.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: 7528, Parent PID: 7520

General

Target ID:	1
Start time:	14:21:57
Start date:	08/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: aspnet_regiis.exe PID: **7596**, Parent PID: **7520**

General

Target ID:	2
Start time:	14:21:57
Start date:	08/06/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe"
Imagebase:	0x10000
File size:	43'016 bytes
MD5 hash:	5D1D74198D75640E889F0A577BBF31FC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Stealc, Description: Yara detected Stealc, Source: 00000002.00000002.1806482282.0000000002BA7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000002.00000002.1805843043.0000000002750000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MarsStealer, Description: Yara detected Mars stealer, Source: 00000002.00000002.1805843043.0000000002750000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.1806482282.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2754ADE	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	2754ADE	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	2754ADE	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	2754ADE	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	2754ADE	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2754ADE	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	2754ADE	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	2754ADE	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	2754ADE	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	2754ADE	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	2754ADE	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	2754ADE	HttpSendRequestA
C:\ProgramData\AFIIEBGCAAECBGCBGCBKEHIJEB	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	275A150	CopyFileA
C:\ProgramData\AFIIEBGCAAECBGCBGCBK	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	2759BB7	CopyFileA
C:\ProgramData\KJJJJDHI	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	275BD0F	CopyFileA
C:\ProgramData\ECAKKKKJDBKKFIEBKEHD	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	2759BB7	CopyFileA
C:\ProgramData\BFHJECAA	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	275BD0F	CopyFileA
C:\ProgramData\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2755E59	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2755E59	CreateFileA
C:\ProgramData\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2755E59	CreateFileA
C:\ProgramData\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2755E59	CreateFileA
C:\ProgramData\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2755E59	CreateFileA
C:\ProgramData\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2755E59	CreateFileA
C:\ProgramData\JEHIDHDAKJDHJKEBFIEHCAAEHD	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	275C6D9	CopyFileA
C:\ProgramData\ECAKKKKJDBKKFIEBKEHDGCAFCB	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	275CF47	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\AFIIEBGCAAECBGCBGCBKEHIJEB	success or wait	1	275A68F	DeleteFileA
C:\ProgramData\AFIIEBGCAAECBGCBGCBK	success or wait	1	2759FF1	DeleteFileA
C:\ProgramData\KJJJJDHI	success or wait	1	275BE38	DeleteFileA
C:\ProgramData\ECAKKKKJDBKKFIEBKEHD	success or wait	1	2759FF1	DeleteFileA
C:\ProgramData\BFHJECAA	success or wait	1	275BE38	DeleteFileA
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\cookies.sqlite-shm	success or wait	1	61E345D4	DeleteFileW
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\cookies.sqlite-wal	success or wait	1	61E345D4	DeleteFileW
C:\ProgramData\JEHIDHDAKJDHJKEBFIEHCAAEHD	success or wait	1	275CB04	DeleteFileA
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\places.sqlite-shm	success or wait	1	61E345D4	DeleteFileW
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\places.sqlite-wal	success or wait	1	61E345D4	DeleteFileW
C:\ProgramData\ECAKKKKJDBKKFIEBKEHDGCAFCB	success or wait	1	275D172	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\AFIIEBGCAAECBGCBGCBKEHIJEB	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 00 00 0b 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	275A150	CopyFileA
C:\ProgramData\AFIIEBGCAAECBGCBGCBK	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	2759BB7	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\KJJJJDHI	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	SQLite format 3@ 4!.j1	success or wait	2	275BD0F	CopyFileA
C:\ProgramData\ECAKKKKJDBKKFIEBKEHD	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	SQLite format 3@ .O}	success or wait	1	2759BB7	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\freebl3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	572	2755E82	InternetReadFile
C:\ProgramData\freebl3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	670	2755EB0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\mozglue[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	561	2755E82	InternetReadFile
C:\ProgramData\mozglue.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	594	2755EB0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\msvcp140[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 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	427	2755E82	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\freebl3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	440	2755EB0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\nss3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1981	2755E82	InternetReadFile
C:\ProgramData\nss3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1999	2755EB0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\softokn3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	252	2755E82	InternetReadFile
C:\ProgramData\softokn3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	252	2755EB0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\vcruntime140[1].dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"	success or wait	79	2755E82	InternetReadFile
C:\ProgramData\vcruntime140.dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"	success or wait	79	2755EB0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\JEHIDHDAKJDHJKEBFIEHCAAEHD	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	1	275C6D9	CopyFileA
C:\ProgramData\ECAKKKKJDBKKFIEBKEHDGCAFCB	0	524288	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAs qpqp{ooh nnemn,m9lklPjjhhgdcc6b baa>	success or wait	10	275CF47	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	2759440	ReadFile
C:\ProgramData\AFIIEBGCAAECBGCBGCBKEHIJEB	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\AFIIEBGCAAECBGCBGCBKEHIJEB	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\AFIIEBGCAAECBGCBGCBKEHIJEB	24	16	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	100	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\AFIIEBGCAAECBGCBGCBK	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\AFIIEBGCAAECBGCBGCBK	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\KJJJJDHI	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\KJJJJDHI	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\KJJJJDHI	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\KJJJJDHI	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\KJJJJDHI	0	100	success or wait	1	61E33FB7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	2759440	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History	0	100	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\ECAKKKKJDBKKFIEBKEHD	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\ECAKKKKJDBKKFIEBKEHD	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\BFHJECAA	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\BFHJECAA	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\BFHJECAA	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\BFHJECAA	0	2048	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\cookies.sqlite	0	100	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\cookies.sqlite	0	32768	success or wait	2	61E33FB7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\cookies.sqlite	32768	32768	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\places.sqlite	0	100	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\places.sqlite	0	32768	success or wait	2	61E33FB7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\fqs92o4p.default-release\places.sqlite	1474560	32768	success or wait	1	61E33FB7	ReadFile

Disassembly

No disassembly