ID: 1436574
Sample Name: FFAk2gixx5.exe
Cookbook: default.jbs
Time: 02:51:03
Date: 06/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

Table of Contents 2
Windows Analysis Report FFAk2gixx5.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 5
Threatname: Vidar 5
Yara Signatures 5
PCAP (Network Traffic) 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Compliance 7
Networking 7
System Summary 7
Data Obfuscation 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 14
Public IPs 14
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\ProgramData\CGDGHCBGDHJJKECAECBA 15
C:\ProgramData\DBFIDGII 16
C:\ProgramData\FCGIJKJJKEBGHJKFIDGCAAFCAF 16
C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG 16
C:\ProgramData\JECBGCFHCFIDHIDHDGDG 17
C:\ProgramData\JEHIJDGI 17
C:\ProgramData\freebl3.dll 17
C:\ProgramData\mozglue.dll 18
C:\ProgramData\msvcp140.dll 18
C:\ProgramData\nss3.dll 18
C:\ProgramData\softokn3.dll 19
C:\ProgramData\vcruntime140.dll 19
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\freebl3[1].dll 19
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\mozglue[1].dll 20
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\msvcp140[1].dll 20
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\nss3[1].dll 20

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\softokn3[1].dll 21
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\vcruntime140[1].dll 21
Static File Info 21
General 21
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 22
Rich Headers 23
Data Directories 23
Sections 24
Resources 24
Imports 25
Possible Origin 25
Network Behavior 26
Snort IDS Alerts 26
Network Port Distribution 26
TCP Packets 26
UDP Packets 28
DNS Queries 28
DNS Answers 28
HTTP Request Dependency Graph 28
Statistics 28
System Behavior 28
Analysis Process: FFAk2gixx5.exePID: 6784, Parent PID: 4004 28
General 28
File Activities 29
File Created 29
File Deleted 31
File Written 31
File Read 40
Disassembly 40

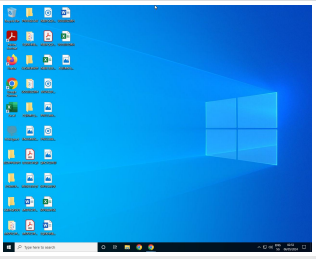
Windows Analysis Report

FFAk2gixx5.exe

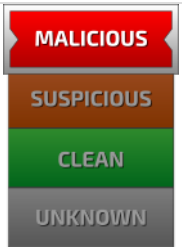
Overview

General Information

Sample name:	FFAk2gixx5.exerenamed because original name is a hash value
Original sample name:	14cd6d9cbad8…
Analysis ID:	1436574
MD5:	14cd6d9cbad8…
SHA1:	6f553fad2fd973..
SHA256:	1738d5ec9cf4a..
Tags:	exe Stealc
Infos:	



Detection



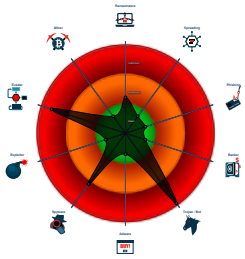
Mars Stealer, Stealc, Vidar

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Yara detected Mars stealer
- Yara detected Stealc
- Yara detected Vidar stealer
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- FFAk2gixx5.exe (PID: 6784 cmdline: "C:\Users\user\Desktop\FFAk2gixx5.exe" MD5: 14CD6D9CBAD80B0E4076212BF7AD937F)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	**http**://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	**http**://https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

Threatname: Vidar


```
{
  "C2 url": "http://okkolus.com/cf5cbdf706840b3f.php"
}
```


Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.3315854062.0000000002FC0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000002.3315854062.0000000002FC0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_MarsStealer	Yara detected Mars stealer	Joe Security	
00000000.00000002.3315657325.0000000002C37000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1208:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.3315706201.0000000002C4C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Stealc	Yara detected Stealc	Joe Security	
00000000.00000002.3314009365.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.FFAk2gixx5.exe.2fc0e67.2.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.FFAk2gixx5.exe.2fc0e67.2.unpack	JoeSecurity_MarsStealer	Yara detected Mars stealer	Joe Security	
0.2.FFAk2gixx5.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.FFAk2gixx5.exe.400000.0.raw.unpack	JoeSecurity_MarsStealer	Yara detected Mars stealer	Joe Security	
0.3.FFAk2gixx5.exe.2ff0000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 7 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/Stealc/Vidar Stealer Active C2 Responding with plugins Config M1 - Source IP: 31.41.44.147 - Destination IP: 192.168.2.6

Timestamp:	05/06/24-02:52:39.695594
SID:	2051831
Source Port:	80
Destination Port:	49708
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Stealc Requesting browsers Config from C2 - Source IP: 192.168.2.6 - Destination IP: 31.41.44.147

Timestamp:	05/06/24-02:52:38.714464
SID:	2044244
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Stealc Active C2 Responding with browsers Config M1 - Source IP: 31.41.44.147 - Destination IP: 192.168.2.6

Timestamp:	05/06/24-02:52:39.070096
SID:	2051828
Source Port:	80
Destination Port:	49707
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Stealc Requesting plugins Config from C2 - Source IP: 192.168.2.6 - Destination IP: 31.41.44.147

Timestamp:	05/06/24-02:52:39.336133
SID:	2044246
Source Port:	49708
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [SEKOIA.IO] Win32/Stealc C2 Check-in - Source IP: 192.168.2.6 - Destination IP: 31.41.44.147

Timestamp:	05/06/24-02:52:38.047891
SID:	2044243
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Sample uses string decryption to hide its real strings

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking locale)

HIPS / PFW / Operating System Protection Evasion

Searches for specific processes (likely to inject)

Stealing of Sensitive Information

Yara detected Mars stealer

Yara detected Stealc

Yara detected Vidar stealer

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

Remote Access Functionality

Yara detected Mars stealer

Yara detected Stealc

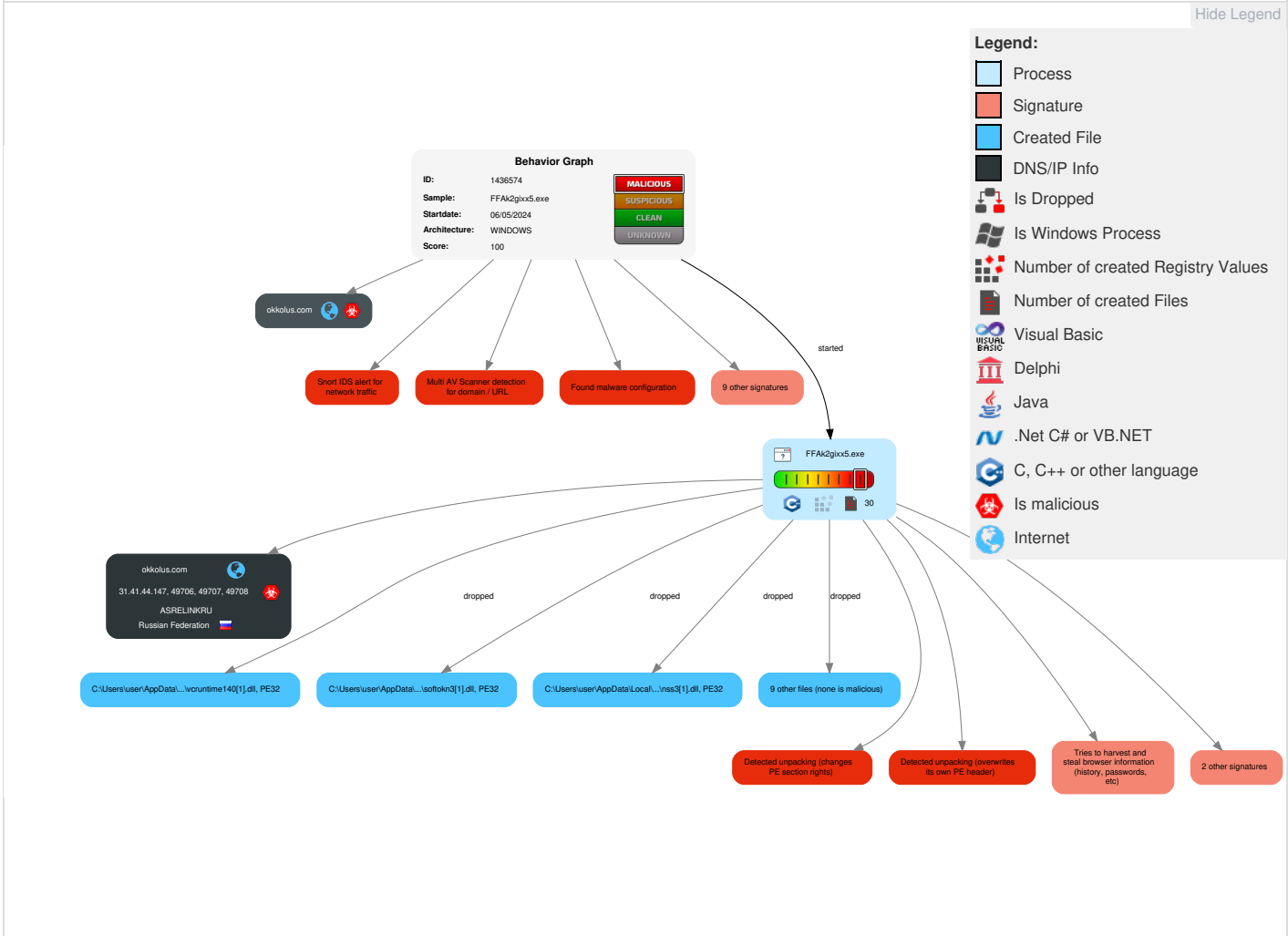
Yara detected Vidar stealer

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 1 Native API	1 DLL Side-Loading	1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	1 Data from Local System	1 2 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service

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

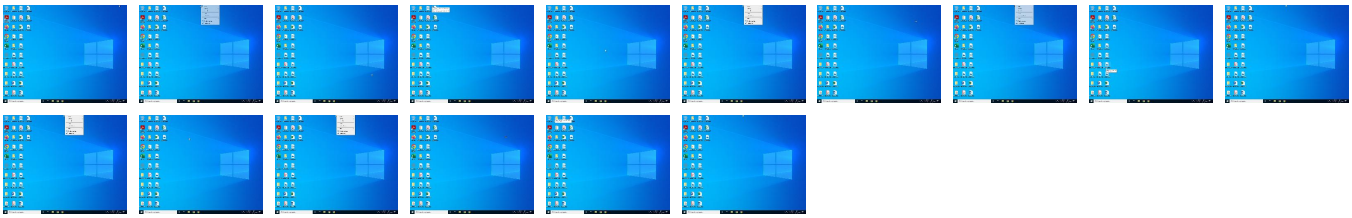
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FFAk2gixx5.exe	71%	ReversingLabs	Win32.Trojan.Stealc	
FFAk2gixx5.exe	68%	Virustotal		Browse
FFAk2gixx5.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	5%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\freebl3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\mozglue[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\msvcp140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\nss3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\softokn3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\vcruntime140[1].dll	5%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
okkolus.com	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://mozilla.org0/	0%	URL Reputation	safe	
http://https://ac.ecopnacl	0%	URL Reputation	safe	
http://https://ac.ecop	0%	URL Reputation	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dllll	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/vcruntime140.dllata	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/msvcp140.dlluPh	0%	Avira URL Cloud	safe	
http://okkolus.com	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/msvcp140.dll.	0%	Avira URL Cloud	safe	
http://okkolus.com	11%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/softokn3.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dll.U	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/mozglue.dllrowser	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dllll	1%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/mozglue.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.php&)	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/mozglue.dll94eaf2a9d1d275a40e443fa5Extension	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/mozglue.dllVUG	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/softokn3.dll	1%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/nss3.dllpatible_edge_version_number	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/softokn3.dller	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dlle	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/freebl3.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/mozglue.dll	3%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/ra	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/msvcp140.dller	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.phpN	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/freebl3.dll	3%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.phpte3.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/vcruntime140.dll	1%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/softokn3.dll.	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://okkolus.com/dfaf16606234b71d/	1%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/softokn3.dllCSF	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dllll_TH	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.phpte3.dll	4%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/freebl3.dll94eaf2a9d1d275a40e443fa5tionComponent	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.phpN	4%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/oTab	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/mozglue.dllser	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/soft	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/softokn3.dller	1%	Virustotal		Browse
http://okkolus.com/cf5cbdf706840b3f.php	100%	Avira URL Cloud	malware	
http://okkolus.com/cf5cbdf706840b3f.php6c3c10c894eaf2a9d1d275a40e443fa5cations	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/vcruntime140.dll%	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dll9M	0%	Avira URL Cloud	safe	
http://okkolus.comppData	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.php	13%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/msvcp140.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/sqlite3.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dlle	5%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/nss3.dll	0%	Avira URL Cloud	safe	
http://okkolus.com/cf5cbdf706840b3f.php/M	100%	Avira URL Cloud	malware	
http://okkolus.com/cf5cbdf706840b3f.phpt	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dllJT	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dlloU	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dll	3%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/mozglue.dlld	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/nss3.dllllx	0%	Avira URL Cloud	safe	
http://okkolus.com/dfaf16606234b71d/sqlite3.dll	4%	Virustotal		Browse
http://okkolus.com/dfaf16606234b71d/msvcp140.dll	3%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
okkolus.com	31.41.44.147	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

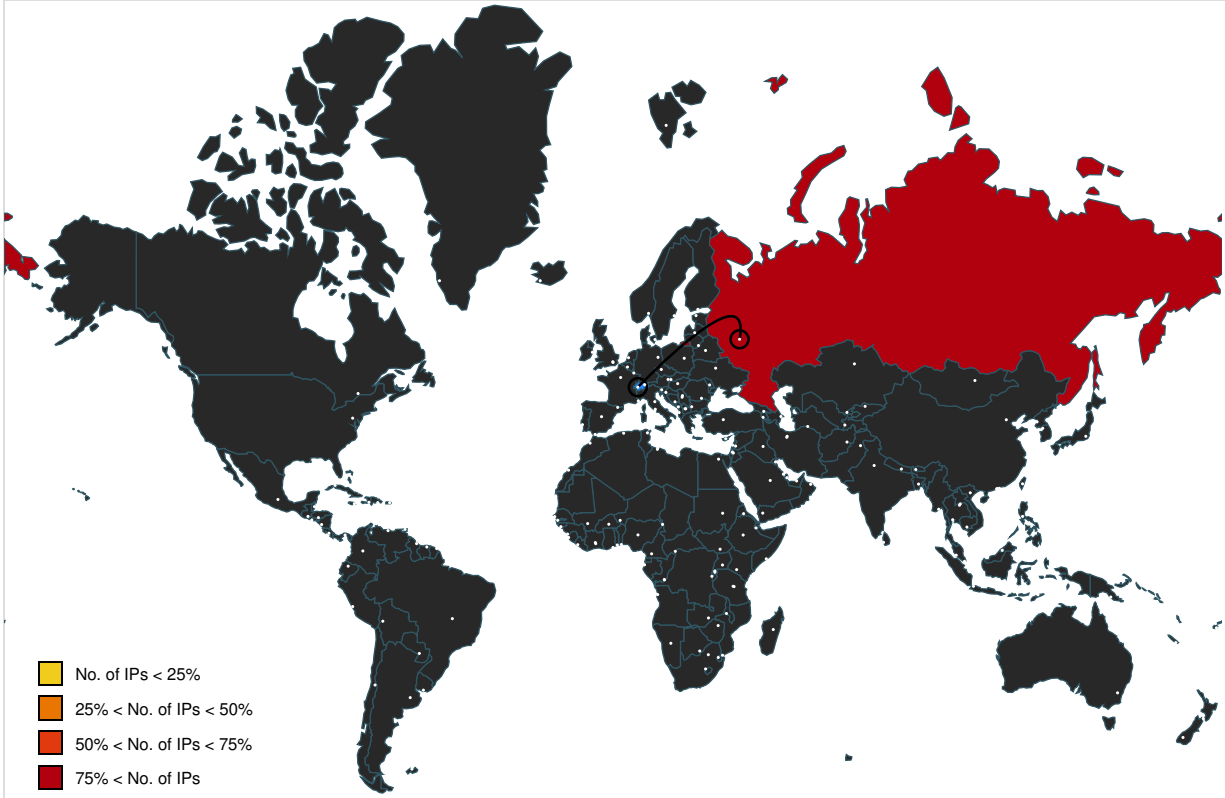
Name	Malicious	Antivirus Detection	Reputation
http://okkolus.com/dfaf16606234b71d/softokn3.dll	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/mozglue.dll	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/freebl3.dll	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/vcruntime140.dll	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/cf5cbdf706840b3f.php	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://okkolus.com/dfaf16606234b71d/msvcp140.dll	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/sqlite3.dll	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dll	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://okkolus.com/dfaf16606234b71d/msvcp140.dlluPh	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002C87000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002C4C000.00000004.00000020.00020000.00000000.sdmp, FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	JEHIJDGI.0.dr	false		high
http://https://duckduckgo.com/ac/?q=	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp, JEHIJDGI.0.dr	false		high
http://okkolus.com/dfaf16606234b71d/vcruntime140.dllata	FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/msvcp140.dll.	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002C87000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dllll	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp, FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002C87000.00000004.00000020.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/cf5cbdf706840b3f.	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dll.U	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp, JEHIJDGI.0.dr	false		high
http://okkolus.com/dfaf16606234b71d/mozglue.dllrowser	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002C87000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/cf5cbdf706840b3f.php&)	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CA4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/mozglue.dll94eaf2a9d1d275a40e443fa5Extension	FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/mozglue.dllVUG	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dllpatible_edge_version_number	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002CAB000.00000004.00000020.00020000.00000000.sdmp, JEHIJDGI.0.dr	false		high
http://okkolus.com/dfaf16606234b71d/softokn3.dller	FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dlle	FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/ra	FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	FFAk2gixx5.exe, 00000000.00000002.3326407277.000000001D119000.00000004.00000020.00020000.00000000.sdmp, FFAk2gixx5.exe, 00000000.00000002.3334018362.0000000061ED3000.00000004.00001000.00020000.00000000.sdmp	false		high
http://okkolus.com/dfaf16606234b71d/msvcp140.dller	FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/cf5cbdf706840b3f.phpN	FFAk2gixx5.exe, 00000000.00000002.3315706201.0000000002C4C000.00000004.00000020.00020000.00000000.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.mozilla.com/en-US/blocklist/	mozglue[1].dll.0.dr, mozglue.dll.0.dr	false		high
http://okkolus.com/dfaf16606234b71d/	FFAk2gixx5.exe, 00000000.00000002.3314009365.0000000000447000.00000040.00000001.01000000.00000003.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mozilla.org0/	freebl3[1].dll.0.dr, softokn3[1].dll.0.dr, freebl3.dll.0.dr, mozglue[1].dll.0.dr, mozglue.dll.0.dr, softokn3.dll.0.dr	false	• URL Reputation: safe	unknown
http://okkolus.com/cf5cbdf706840b3f.phpte3.dll	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000549000.00000040.00000001. 01000000.00000003.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/softokn3.dll.	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002C87000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/softokn3.dllCSF	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002C87000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	JEHIJDGI.0.dr	false		high
http://okkolus.com/dfaf16606234b71d/nss3.dllll_TH	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/freebl3.dll94eaf2a9d1d275a40e443fa5tionComponent	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000447000.00000040.00000001. 01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/oTab	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000447000.00000040.00000001. 01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/mozglue.dllser	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000447000.00000040.00000001. 01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp, JEHIJDGI.0.dr	false		high
http://okkolus.com/dfaf16606234b71d/soft	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000447000.00000040.00000001. 01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/cf5cbdf706840b3f.php6c3c10c894eaf2a9d1d275a40e443fa5cations	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000447000.00000040.00000001. 01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/vcruntime140.dll%	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	JEHIJDGI.0.dr	false		high
http://okkolus.com/dfaf16606234b71d/nss3.dll9M	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.comppData	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000447000.00000040.00000001. 01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	JEHIJDGI.0.dr	false		high
http://https://ac.ecopnacl	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://okkolus.com/cf5cbdf706840b3f.php/M	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://okkolus.com/cf5cbdf706840b3f.phpt	FFAk2gixx5.exe, 00000000.00000002.331400 9365.0000000000447000.00000040.00000001. 01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dllJT	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dlloU	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecop	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002CAB000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://okkolus.com/dfaf16606234b71d/mozglue.dlld	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002C87000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://okkolus.com/dfaf16606234b71d/nss3.dllllx	FFAk2gixx5.exe, 00000000.00000002.331570 6201.0000000002C87000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	JEHIJDGI.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.41.44.147	okkolus.com	Russian Federation		56577	ASRELINKRU	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1436574
Start date and time:	2024-05-06 02:51:03 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	FFAk2gixx5.exerenamed because original name is a hash value
Original Sample Name:	14cd6d9cbad80b0e4076212bf7ad937f.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/18@1/1
EGA Information:	• Successful, ratio: 100%

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- HTTP raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\CGDGHCBGDHJJKECAECBA

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4

SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j..... ....

C:\ProgramData\DBFIDGII

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W..... ....

C:\ProgramData\FCGIJKJJKEBGHJKFIDGCAAFCAF

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j...$.....g..... ....

C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 6, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 6
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8508558324143882
Encrypted:	false
SSDEEP:	24:TLlF1kwNbXYFpFNYcw+6UwcQVXH5fBaJvWKC0ABndzGrW7swaE:TxFawNLopFgU10XJBaEKQxdgQsw
MD5:	933D6D14518371B212F36C3835794D75
SHA1:	92D056D912B3C0260D379330D3CC0359B57A322B
SHA-256:	55390EE61FB85370A8A7F51A8DD5374F7B1801D1D7DF09D6A90CDD74ED6E7D1E
SHA-512:	EAC706D8A579500EADA26FB9883E1F3CE9112A03F38EE78B11B393AB0A3285945F8E06EB406BFC17D1CB540F840E435E515FABFC265399CE6F5193980FDE3F2C
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	SQLite format 3.....@ .....j.....g...$.....

C:\ProgramData\JECBGCFHCFIDHIDHDGDG

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 2, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8745947603342119
Encrypted:	false
SSDEEP:	96:aZ8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:W8yLG7IwRWf4
MD5:	378391FDB591852E472D99DC4BF837DA
SHA1:	10CB2CDAD4EDCCACE0A7748005F52C5251F6F0E0
SHA-256:	513C63B0E44FFDE2B4E511A69436799A8B59585CB0EB5CCFDA7A9A8F06BA4808
SHA-512:	F099631BEC265A6E8E4F8808270B57FFF28D7CBF75CC6FA046BB516E8863F36E8506C7A38AD682132FCB1134D26326A58F5B588B9EC9604F09FD7155B2AEF2D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....j.....

C:\ProgramData\JEHIJDGI

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4
MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB00114 9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\ProgramData\freebl3.dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	685392
Entropy (8bit):	6.872871740790978
Encrypted:	false
SSDEEP:	12288:4gPbPpxMofhPNN0+RXBrp3M5pzRN4l2SQ+PEu9tUs/abAQb51FW/IzkOfWPO9UN7:4gPbPp9NNP0BgInfW2WMC4M+hW
MD5:	550686C0EE48C386DFCB40199BD076AC
SHA1:	EE5134DA4D3EFCB466081FB6197BE5E12A5B22AB
SHA-256:	EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
SHA-512:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....4.....p.....@A.... .....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F.. .0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..."..... .....@..B.....

C:\ProgramData\mozglue.dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.833616094889818
Encrypted:	false
SSDEEP:	12288:BlSyAom/gcRKMdRm4wFkRHuyG4RRGJVDjMk/x21R8gY/r:BKgcRKMdRm4wFkVVDGJVv//x21R8br
MD5:	C8FD9BE83BC728CC04BEFFAFC2907FE9
SHA1:	95AB9F701E0024CEDFBD312BCFE4E726744C4F2E
SHA-256:	BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
SHA-512:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B 40
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....^.....j.....@A.... .....`...W.....P/...0...A...S.....h.....Z.....text...a..... ..`.rdata.....@..@.data...D..... .....@....00cfg.....@..@.tls.....@....rsrc..... .....@..@.reloc...A...0...B.....@..B.....

C:\ProgramData\msvcp140.dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	450024
Entropy (8bit):	6.673992339875127
Encrypted:	false
SSDEEP:	12288:McPa9C9VbL+3Omy5CvyOvzeOKdqhUgiW6QR7t5s03Ooc8dHkC2esGAWf:McPa90Vbky5CvyUeOKn03Ooc8dHkC2eN
MD5:	5FF1FCA37C466D6723EC67BE93B51442
SHA1:	34CC4E158092083B13D67D6D2BC9E57B798A303B
SHA-256:	5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
SHA-512:	4802EF62630C521D83A1D333969593FB00C9B38F82B4D07F70FBD21F495FEA9B3F67676064573D2C71C42BC6F7019929897422135 01B16087BB6110E337C7546
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._...._...._)n...._....._...^."._..^..._..\..._..[..._..Z..._..._..._.....]..._.Rich.._.....PE..L.....0].....!....(.....`.....@.....,.....@A.....g.....r.....A.....=..`x..8.....w ..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc..... .....Z.....@..@.reloc...=.....>...^.....@..B.....

C:\ProgramData\nss3.dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1815519
Entropy (8bit):	6.634812314798213
Encrypted:	false
SSDEEP:	49152:fECf12gikHlnKGxJRIB+y5nvxnaOSJ3HFNWYrVvE4CQsgzMmQfTU1NrWmy4KoAzo:J7Tf8J1Q+q
MD5:	7D191EE364B1851D2E42F34E609B9C20
SHA1:	8D2396AF483E19522D500984908F854D61A04A44
SHA-256:	724F186341F020B14781246C5CEB26962C18D322F4C96439EFA7BBE28D151DE7
SHA-512:	A1BC8DCDB1E64C000134440B122B898549B46C1F2E928C4DCC073AC3E04FD7B3D9375A7A87E900238749BFABDC17E1E4C7CF6644F1F37853D3696CB04C9ED7 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....`.....p.....l- ...@A.... .....&.....@....P..x.....P/...`..\.....\....&..@.....text..... ..`.rdata..l.....@..@.data...DR.. .....@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\...`.....@..B..... ....

C:\ProgramData\softokn3.dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	257872
Entropy (8bit):	6.727482641240852
Encrypted:	false
SSDEEP:	6144:/yF/zX2zfRkU62THVh/T2AhZxv6A31obD6Hq/8jis+FvtVRpsAAs0o8OqTYz+xnU:/yRzX2zfRkX2T1h/SA5PF9m8jJqKYz+y
MD5:	4E52D739C324DB8225BD9AB2695F262F
SHA1:	71C3DA43DC5A0D2A1941E874A6D015A071783889
SHA-256:	74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
SHA-512:	2D4168A69082A9192B9248F7331BD806C260478FF817567DF54F997D7C3C7D640776131355401E4BDB9744E246C36D658CB24B18DE67D8F23F10066E5FE445F6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....P.....Sg ....@A.....Dv..S....w.....P/.....5..8q.....{.....text...&..... ..`.rdata.....@..@.da ta.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... ....

C:\ProgramData\vcruntime140.dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55296
Entropy (8bit):	6.558106649929844
Encrypted:	false
SSDEEP:	768:lK+3U7KL+LAPRycNr1gyIjFxv5ePM5et/jw1UgS05/w7uxgczc74BuRJNd6NRJ3M:lw2886xv555et/MCsjw0BuRK3jteoe
MD5:	ABE1198FEA554BA7456D12709E9C788D
SHA1:	1DE434DCFA780C88A75EC3502A9CE6363D05943B
SHA-256:	1776DF92E6C198A7360F1EB13ECAD1630DFA0655CB9E52C086EFB9503277C9F6
SHA-512:	1A531FA1CD3EDD1C78B8655A2E2FA9A183E2196141F56ED2C398C1FD6E1BDF39DD572AEEFD9FD211158A32311F7B0484085A7DEA5FB749895D00C08EA20BA9 D6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 5%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... ......PE..L...|.0]....."!.....0.....m....@A.....A... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\freebl3[1].dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	685392
Entropy (8bit):	6.872871740790978
Encrypted:	false
SSDEEP:	12288:4gPbPpxMofhPNN0+RXBrp3M5pzRN4l2SQ+PEu9tUs/abAQb51FW/IzkOfWPO9UN7:4gPbPp9NNP0BgInfW2WMC4M+hW
MD5:	550686C0EE48C386DFCB40199BD076AC
SHA1:	EE5134DA4D3EFCB466081FB6197BE5E12A5B22AB
SHA-256:	EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
SHA-512:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....4.....p.....@A.... .....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F.. .0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..."..... .....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\mozglue[1].dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.833616094889818
Encrypted:	false
SSDEEP:	12288:BlSyAom/gcRKMdRm4wFkRHuyG4RRGJVDjMk/x21R8gY/r:BKgcRKMdRm4wFkVVDGJVv//x21R8br
MD5:	C8FD9BE83BC728CC04BEFFAFC2907FE9
SHA1:	95AB9F701E0024CEDFBD312BCFE4E726744C4F2E
SHA-256:	BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
SHA-512:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B 40
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....^.....j.....@A.... .....`...W.....P/...0...A...S.....h.....Z.....text...a..... ..`.rdata.....@..@.data...D..... .....@....00cfg.....@..@.tls.....@....rsrc..... .....@..@.reloc...A...0...B.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\msvcp140[1].dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	450024
Entropy (8bit):	6.673992339875127
Encrypted:	false
SSDEEP:	12288:McPa9C9VbL+3Omy5CvyOvzeOKdqhUgiW6QR7t5s03Ooc8dHkC2esGAWf:McPa90Vbky5CvyUeOKn03Ooc8dHkC2eN
MD5:	5FF1FCA37C466D6723EC67BE93B51442
SHA1:	34CC4E158092083B13D67D6D2BC9E57B798A303B
SHA-256:	5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
SHA-512:	4802EF62630C521D83A1D333969593FB00C9B38F82B4D07F70FBD21F495FEA9B3F67676064573D2C71C42BC6F7019929897422135 01B16087BB6110E337C7546
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._...._...._)n...._....._...^."._..^..._..\..._..[..._..Z..._..._..._.....]..._.Rich.._.....PE..L.....0].....!....(.....`.....@.....,....@A.....g.....r.....A.....=..`x..8.....w ..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc..... .....Z.....@..@.reloc...=.....>...^.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\nss3[1].dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1815519
Entropy (8bit):	6.634812314798213
Encrypted:	false
SSDEEP:	49152:fECf12gikHlnKGxJRIB+y5nvxnaOSJ3HFNWYrVvE4CQsgzMmQfTU1NrWmy4KoAzo:J7Tf8J1Q+q
MD5:	7D191EE364B1851D2E42F34E609B9C20
SHA1:	8D2396AF483E19522D500984908F854D61A04A44
SHA-256:	724F186341F020B14781246C5CEB26962C18D322F4C96439EFA7BBE28D151DE7
SHA-512:	A1BC8DCDB1E64C000134440B122B898549B46C1F2E928C4DCC073AC3E04FD7B3D9375A7A87E900238749BFABDC17E1E4C7CF6644F1F37853D3696CB04C9ED7 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....`.....p.....l- ...@A.....&.....@....P..x.....P/...`..\.....\....&..@.....text..... ..`.rdata..l.....@..@.data...DR.. .....@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\...`.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\softokn3[1].dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	257872
Entropy (8bit):	6.727482641240852
Encrypted:	false
SSDEEP:	6144:/yF/zX2zfRkU62THVh/T2AhZxv6A31obD6Hq/8jis+FvtVRpsAAs0o8OqTYz+xnU:/yRzX2zfRkX2T1h/SA5PF9m8jJqKYz+y
MD5:	4E52D739C324DB8225BD9AB2695F262F
SHA1:	71C3DA43DC5A0D2A1941E874A6D015A071783889
SHA-256:	74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
SHA-512:	2D4168A69082A9192B9248F7331BD806C260478FF817567DF54F997D7C3C7D640776131355401E4BDB9744E246C36D658CB24B18DE67D8F23F10066E5FE445F6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....P.....Sg ....@A.....Dv..S....w.....P/.....5..8q.....{.....text...&..... ..`.rdata.....@..@.da ta.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\vcruntime140[1].dll

Process:	C:\Users\user\Desktop\FFAk2gixx5.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55296
Entropy (8bit):	6.558106649929844
Encrypted:	false
SSDEEP:	768:lK+3U7KL+LAPRycNr1gyIjFxv5ePM5et/jw1UgS05/w7uxgczc74BuRJNd6NRJ3M:lw2886xv555et/MCsjw0BuRK3jteoe
MD5:	ABE1198FEA554BA7456D12709E9C788D
SHA1:	1DE434DCFA780C88A75EC3502A9CE6363D05943B
SHA-256:	1776DF92E6C198A7360F1EB13ECAD1630DFA0655CB9E52C086EFB9503277C9F6
SHA-512:	1A531FA1CD3EDD1C78B8655A2E2FA9A183E2196141F56ED2C398C1FD6E1BDF39DD572AEEFD9FD211158A32311F7B0484085A7DEA5FB749895D00C08EA20BA9 D6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 5%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L...|.0]....."!.....0.....m....@A.....A... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.920409946909827
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:	FFAk2gixx5.exe
File size:	296'960 bytes
MD5:	14cd6d9cbad80b0e4076212bf7ad937f
SHA1:	6f553fad2fd973d52dec55582490eb8c3a35b6e1
SHA256:	1738d5ec9cf4a62d3bebdb8690d208dc4e9bb957ba427233920a2195b04bb52e
SHA512:	ca8e1d03dec6ec41eba8b169ef3ce70a1f0acde0c0a9592d99f0d0013577647826a1711ef923b19bb00abc0a87cca240a042f3a237cec13ded5793519d7d56cf

SSDEEP:	3072:89dR4sFy2KJnd64kX/qCdx7Hto4r7uYl4HN+5BOlmXvg1T/dO:89dR4I58ndnkXiCpTeYl4HNyO8XYt/w
TLSH:	9F549E002590E823DF964771591DCEE0662FBC618BF4929E7214379F29B31A2712EB7F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x2...a...a...a...a...a...a...a...a...a.dma...a...a...a...a...a...a...a...aRich...a.....PE..L...320d.....

File Icon

Icon Hash:	1321252d29170f17

Static PE Info

General

Entrypoint:	0x401604
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x64303233 [Fri Apr 7 15:09:39 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	be37cfa8808e82b62b6ce7f603a1d7f3

Entrypoint Preview

Instruction
call 00007FD2917FD7C8h
jmp 00007FD2917F9D2Dh
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007FD2917F9ED6h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007FD2917F9F00h
test ecx, 00000003h
jne 00007FD2917F9EA1h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007FD2917F9E9Ah
mov eax, dword ptr [ecx-04h]
test al, al

Instruction
je 00007FD2917F9EE4h
test ah, ah
je 00007FD2917F9ED6h
test eax, 00FF0000h
je 00007FD2917F9EC5h
test eax, FF000000h
je 00007FD2917F9EB4h
jmp 00007FD2917F9E7Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 0040C204h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi
test eax, eax
je 00007FD2917F9EBEh
test byte ptr [eax], 00000008h
je 00007FD2917F9EB9h
mov dword ptr [ebp-0Ch], 00000000h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2efcc	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26ee000	0x17a00	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xc000	0x18c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa7b3	0xa800	a348b7fef0847937bda16a227a110ac4	False	0.6162574404761905	data	6.584458478900951	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xc000	0x238ca	0x23a00	63652be27cb3906220238ec6760801ed	False	0.6058799342105263	data	5.920319471747451	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x30000	0x26bd33c	0x2800	e97657bf7ad1ab2806f27164f93ba97d	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x26ee000	0x17a00	0x17a00	a862c21bfacd8f779ede71e4ac914e7e	False	0.43974247685185186	data	5.043845287134813	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
GABUWOCEMOXOXATAZIWIV	0x2701040	0x476	ASCII text, with very long lines (1142), with no line terminators	Turkish	Turkey	0.626970227670753
RT_CURSOR	0x27014d8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0			0.31023454157782515
RT_CURSOR	0x2702398	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0			0.7368421052631579
RT_CURSOR	0x27024c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0			0.06130705394190871
RT_ICON	0x26ee850	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Turkish	Turkey	0.4157782515991471
RT_ICON	0x26ef6f8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Turkish	Turkey	0.5365523465703971
RT_ICON	0x26effa0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Turkish	Turkey	0.6054147465437788
RT_ICON	0x26f0668	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Turkish	Turkey	0.6575144508670521
RT_ICON	0x26f0bd0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Turkish	Turkey	0.49336099585062243
RT_ICON	0x26f3178	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Turkish	Turkey	0.5117260787992496
RT_ICON	0x26f4220	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Turkish	Turkey	0.5795081967213115
RT_ICON	0x26f4ba8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Turkish	Turkey	0.6090425531914894
RT_ICON	0x26f5088	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Turkish	Turkey	0.39632196162046907
RT_ICON	0x26f5f30	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Turkish	Turkey	0.5185018050541517
RT_ICON	0x26f67d8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Turkish	Turkey	0.581221198156682
RT_ICON	0x26f6ea0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Turkish	Turkey	0.6257225433526011

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x26f7408	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Turkish	Turkey	0.47313278008298754
RT_ICON	0x26f99b0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Turkish	Turkey	0.5278688524590164
RT_ICON	0x26fa338	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Turkish	Turkey	0.5514184397163121
RT_ICON	0x26fa808	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Turkish	Turkey	0.43976545842217485
RT_ICON	0x26fb6b0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Turkish	Turkey	0.5613718411552346
RT_ICON	0x26fbf58	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Turkish	Turkey	0.597926267281106
RT_ICON	0x26fc620	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Turkish	Turkey	0.6604046242774566
RT_ICON	0x26fcb88	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Turkish	Turkey	0.3771784232365145
RT_ICON	0x26ff130	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Turkish	Turkey	0.4022045028142589
RT_ICON	0x27001d8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Turkish	Turkey	0.4266393442622951
RT_ICON	0x2700b60	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Turkish	Turkey	0.4299645390070922
RT_STRING	0x2704c78	0x3f0	data			0.47023809523809523
RT_STRING	0x2705068	0xb6	data			0.5824175824175825
RT_STRING	0x2705120	0x682	data			0.42737094837935174
RT_STRING	0x27057a8	0x156	data			0.5263157894736842
RT_STRING	0x2705900	0xfe	data			0.5433070866141733
RT_ACCELERATOR	0x27014b8	0x20	data			1.09375
RT_GROUP_CURSOR	0x2702380	0x14	data			1.25
RT_GROUP_CURSOR	0x2704a70	0x22	data			1.088235294117647
RT_GROUP_ICON	0x26f5010	0x76	data	Turkish	Turkey	0.6610169491525424
RT_GROUP_ICON	0x26fa7a0	0x68	data	Turkish	Turkey	0.7019230769230769
RT_GROUP_ICON	0x2700fc8	0x76	data	Turkish	Turkey	0.6694915254237288
RT_VERSION	0x2704a98	0x1e0	data			0.5708333333333333

Imports

DLL	Import
KERNEL32.dll	GetCommState, SetDefaultCommConfigW, FreeEnvironmentStringsA, GetModuleHandleW, GetProcessHeap, GetConsoleAliasesLengthA, GetSystemTimes, GetVolumeInformationA, LoadLibraryW, IsBadCodePtr, GetConsoleAliasExesLengthW, lstrcpynW, GetModuleFileNameW, SetConsoleTitleA, SetCurrentDirectoryA, FindFirstFileExA, EnumCalendarInfoW, SetLastError, GetProcAddress, GetLongPathNameA, GetConsoleDisplayMode, SetFileAttributesA, BuildCommDCBW, SetFileApisToOEM, LoadLibraryA, WriteConsoleA, LocalAlloc, SetConsoleCtrlHandler, HeapWalk, FindAtomA, WaitForMultipleObjects, EnumDateFormatsW, GetSystemTime, GetCurrentDirectoryW, GetLocaleInfoA, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, GetLastError, HeapFree, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, SetHandleCount, GetFileType, DeleteCriticalSection, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetFilePointer, GetConsoleCP, GetConsoleMode, EnterCriticalSection, LeaveCriticalSection, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, VirtualAlloc, HeapReAlloc, HeapSize, InitializeCriticalSectionAndSpinCount, SetStdHandle, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, CreateFileA, CloseHandle, FlushFileBuffers
ADVAPI32.dll	ReadEventLogA

Possible Origin

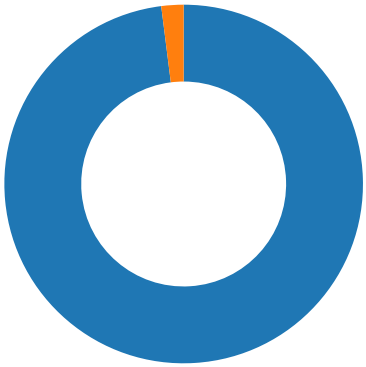
Language of compilation system	Country where language is spoken	Map
Turkish	Turkey	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/06/24-02:52:39.695594	TCP	2051831	ET TROJAN Win32/Stealc/Vidar Stealer Active C2 Responding with plugins Config M1	80	49708	31.41.44.147	192.168.2.6
05/06/24-02:52:38.714464	TCP	2044244	ET TROJAN Win32/Stealc Requesting browsers Config from C2	49707	80	192.168.2.6	31.41.44.147
05/06/24-02:52:39.070096	TCP	2051828	ET TROJAN Win32/Stealc Active C2 Responding with browsers Config M1	80	49707	31.41.44.147	192.168.2.6
05/06/24-02:52:39.336133	TCP	2044246	ET TROJAN Win32/Stealc Requesting plugins Config from C2	49708	80	192.168.2.6	31.41.44.147
05/06/24-02:52:38.047891	TCP	2044243	ET TROJAN [SEKOIA.IO] Win32/Stealc C2 Check-in	49706	80	192.168.2.6	31.41.44.147

Network Port Distribution



Total Packets: 50

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 02:52:37.787518024 CEST	49706	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.046910048 CEST	80	49706	31.41.44.147	192.168.2.6
May 6, 2024 02:52:38.047061920 CEST	49706	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.047890902 CEST	49706	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.351459026 CEST	80	49706	31.41.44.147	192.168.2.6
May 6, 2024 02:52:38.409950972 CEST	80	49706	31.41.44.147	192.168.2.6
May 6, 2024 02:52:38.410156012 CEST	49706	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.411684036 CEST	80	49706	31.41.44.147	192.168.2.6
May 6, 2024 02:52:38.411755085 CEST	49706	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.416929007 CEST	49706	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.436707020 CEST	49707	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.676016092 CEST	80	49706	31.41.44.147	192.168.2.6
May 6, 2024 02:52:38.700299978 CEST	80	49707	31.41.44.147	192.168.2.6
May 6, 2024 02:52:38.700392008 CEST	49707	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:38.714463949 CEST	49707	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.019650936 CEST	80	49707	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.070096016 CEST	80	49707	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.070133924 CEST	80	49707	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.070174932 CEST	49707	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.070200920 CEST	49707	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.070417881 CEST	49707	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.071690083 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.335900068 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.335971117 CEST	49708	80	192.168.2.6	31.41.44.147

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 02:52:39.336133003 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.365117073 CEST	80	49707	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.365191936 CEST	49707	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.643443108 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.695594072 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.695687056 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.695741892 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.695802927 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.877302885 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.877357960 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.920216084 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.920231104 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:39.920264959 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.920303106 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.920681953 CEST	49708	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:39.973120928 CEST	49709	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:40.184652090 CEST	80	49708	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.234769106 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.234877110 CEST	49709	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:40.235045910 CEST	49709	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:40.235097885 CEST	49709	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:40.495630980 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.495649099 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.495814085 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.496064901 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.496180058 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.496381998 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.594436884 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.594455004 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:40.594572067 CEST	49709	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:40.683619022 CEST	49709	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:40.944010019 CEST	80	49709	31.41.44.147	192.168.2.6
May 6, 2024 02:52:43.595019102 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:43.857517958 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:43.857686043 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:43.863915920 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.167375088 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.221414089 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.221450090 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.221497059 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.221517086 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.309515953 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.309644938 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.309648037 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.309703112 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.361118078 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.361227989 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.361238003 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.361273050 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.446191072 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.446211100 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.446225882 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.446239948 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.446289062 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.446316957 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.483799934 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.483870983 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.483947992 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.483959913 CEST	80	49710	31.41.44.147	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 02:52:44.483974934 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.483987093 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.484006882 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.484019041 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.571896076 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.572068930 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.572226048 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.572238922 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.572251081 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.572269917 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.572297096 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.623730898 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.623815060 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.623840094 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.623852015 CEST	80	49710	31.41.44.147	192.168.2.6
May 6, 2024 02:52:44.623882055 CEST	49710	80	192.168.2.6	31.41.44.147
May 6, 2024 02:52:44.623898983 CEST	49710	80	192.168.2.6	31.41.44.147

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 02:52:35.917686939 CEST	57119	53	192.168.2.6	1.1.1.1
May 6, 2024 02:52:36.512387037 CEST	53	57119	1.1.1.1	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 6, 2024 02:52:35.917686939 CEST	192.168.2.6	1.1.1.1	0xce17	Standard query (0)	okkolus.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 6, 2024 02:52:36.512387037 CEST	1.1.1.1	192.168.2.6	0xce17	No error (0)	okkolus.com		31.41.44.147	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- okkolus.com

Statistics

No statistics

System Behavior

Analysis Process: FFAk2gixx5.exe PID: **6784**, Parent PID: **4004**

General

Target ID:	0
Start time:	02:51:48
Start date:	06/05/2024

Path:	C:\Users\user\Desktop\FFAk2gixx5.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FFAk2gixx5.exe"
Imagebase:	0x400000
File size:	296'960 bytes
MD5 hash:	14CD6D9CBAD80B0E4076212BF7AD937F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.3315854062.0000000002FC0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MarsStealer, Description: Yara detected Mars stealer, Source: 00000000.00000002.3315854062.0000000002FC0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.3315657325.0000000002C37000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Stealc, Description: Yara detected Stealc, Source: 00000000.00000002.3315706201.0000000002C4C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.3314009365.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_MarsStealer, Description: Yara detected Mars stealer, Source: 00000000.00000002.3314009365.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.3315854062.0000000002FC0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000003.2531825122.0000000002FF0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MarsStealer, Description: Yara detected Mars stealer, Source: 00000000.00000003.2531825122.0000000002FF0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	false

File Activities

File Created

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	404ADE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	404ADE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	404ADE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	404ADE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	404ADE	HttpSendRequestA
C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG	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	40A150	CopyFileA
C:\ProgramData\CGDGHCBGDHJJKECAECBA	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	409BB7	CopyFileA
C:\ProgramData\JEHIJDGI	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	40BD0F	CopyFileA
C:\ProgramData\FCGIJKJJKEBGHJKFIDGCAAFCAF	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	40A150	CopyFileA
C:\ProgramData\JECBGCFHCFIDHIDHDGDG	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	409BB7	CopyFileA
C:\ProgramData\DBFIDGII	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	40BD0F	CopyFileA
C:\ProgramData\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E59	CreateFileA
C:\ProgramData\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E59	CreateFileA
C:\ProgramData\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E59	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E59	CreateFileA
C:\ProgramData\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E59	CreateFileA
C:\ProgramData\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E59	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG	success or wait	1	40A68F	DeleteFileA
C:\ProgramData\CGDGHCBGDHJJKECAECBA	success or wait	1	409FF1	DeleteFileA
C:\ProgramData\JEHIJDGI	success or wait	1	40BE38	DeleteFileA
C:\ProgramData\FCGIJKJJKEBGHJKFIDGCAAFCAF	success or wait	1	40A68F	DeleteFileA
C:\ProgramData\JECBGCFHCFIDHIDHDGDG	success or wait	1	409FF1	DeleteFileA
C:\ProgramData\DBFIDGII	success or wait	1	40BE38	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG	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 06 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	40A150	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\CGDGHCBGDHJJKECAECBA	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	409BB7	CopyFileA
C:\ProgramData\JEHIJDGI	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	40BD0F	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FCGIJKJJKEBGHJKFIDGCAAFCAF	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 6a fd 0d 0d 24 00 04 0a 0c 00 0f 67 0f fd 0a 0c 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j$g	success or wait	1	40A150	CopyFileA
C:\ProgramData\JECBGCFHCFIDHIDHDGDG	0	51200	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 05 00 00 00 02 07 fd 00 00 00 00 18 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	409BB7	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\DBFIDGII	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 37 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y7.jW	success or wait	2	40BD0F	CopyFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\freebl3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	585	405E82	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\freebl3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	670	405EB0	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\mozglue[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	520	405E82	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\mozglue.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	594	405EB0	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\msvcp140[1].dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	349	405E82	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\msvcp140.dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^_ _[_Z_____]_Rich_	success or wait	440	405EB0	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\nss3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1209	405E82	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\nss3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	1773	405EB0	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\softokn3[1].dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@ADvSw	success or wait	228	405E82	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\softokn3.dll	0	1024	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 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 53 67 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 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@A DvSw	success or wait	252	405EB0	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\vcruntime140[1].dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"	success or wait	54	405E82	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\vcruntime140.dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 0f fd fd fd fd fd fd 0a 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 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"	success or wait	54	405EB0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	66860	success or wait	1	409440	ReadFile
C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\GHJJDGHCBGDHIECBGIDAEHCGDG	24	16	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	100	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\CGDGHCBGDHJJKECAECBA	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\CGDGHCBGDHJJKECAECBA	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JEHIJDGI	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JEHIJDGI	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JEHIJDGI	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JEHIJDGI	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JEHIJDGI	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JEHIJDGI	0	2048	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	44455	success or wait	1	409440	ReadFile
C:\ProgramData\FCGIJKJJKEBGHJKFIDGCAAFCAF	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\FCGIJKJJKEBGHJKFIDGCAAFCAF	0	4096	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History	0	100	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History-journal	0	1	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History	0	4096	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History	94208	4096	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History-journal	0	1	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JECBGCFHCFIDHIDHDGDG	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\JECBGCFHCFIDHIDHDGDG	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\DBFIDGII	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\DBFIDGII	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\DBFIDGII	0	100	success or wait	1	61E33FB7	ReadFile

Disassembly

No disassembly