



ID: 756295
Sample Name: file.exe
Cookbook: default.jbs
Time: 00:09:10
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Vidar 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
System Summary 5
Hooking and other Techniques for Hiding and Protection 5
HIPS / PFW / Operating System Protection Evasion 5
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
C:\ProgramData\102688620397124445057777O8 12
C:\ProgramData\11565709257171813179063097 12
C:\ProgramData\48870274652683548820497570 12
C:\ProgramData\58308559385186415876143610 13
C:\ProgramData\82308976761520470245380715 13
C:\ProgramData\82668342394913559298137947 13
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 15
Data Directories 15
Sections 16
Resources 16
Imports 16
Possible Origin 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 19

DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: file.exePID: 5884, Parent PID: 3320 19
General 19
Analysis Process: file.exePID: 5924, Parent PID: 5884 20
General 20
Analysis Process: file.exePID: 5896, Parent PID: 5924 20
General 20
File Activities 20
Analysis Process: cmd.exePID: 5984, Parent PID: 5896 20
General 20
File Activities 21
Analysis Process: conhost.exePID: 4656, Parent PID: 5984 21
General 21
Analysis Process: timeout.exePID: 3384, Parent PID: 5984 21
General 21
File Activities 21
Disassembly 22

Copyright Joe Security LLC 2022

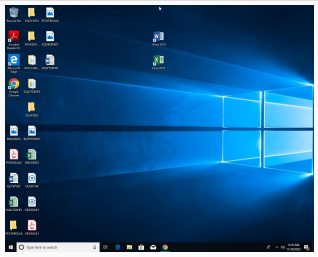
Windows Analysis Report

file.exe

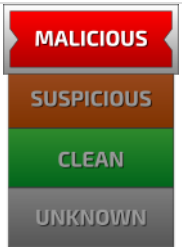
Overview

General Information

Sample Name:	file.exe
Analysis ID:	756295
MD5:	5367709f0a9671..
SHA1:	244bdcc9a35481..
SHA256:	2cc0be582a350f...
Tags:	exe
Infos:	



Detection



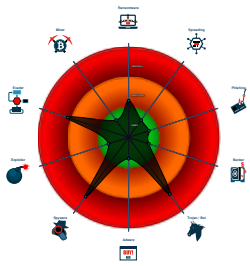
Vidar

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected Vidar stealer
- Tries to steal Crypto Currency Walle...
- Tries to harvest and steal Putty / W...
- Self deletion via cmd or bat file
- Machine Learning detection for sam...
- Injects a PE file into a foreign proce...
- C2 URLs / IPs found in malware con...
- Found many strings related to Crypt...
- Tries to harvest and steal browser in...
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5884 cmdline: C:\Users\user\Desktop\file.exe MD5: 5367709F0A96713B5C9A518E13F306D6)
  - file.exe (PID: 5924 cmdline: C:\Users\user\Desktop\file.exe MD5: 5367709F0A96713B5C9A518E13F306D6)
    - file.exe (PID: 5896 cmdline: C:\Users\user\Desktop\file.exe MD5: 5367709F0A96713B5C9A518E13F306D6)
      - cmd.exe (PID: 5984 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\Desktop\file.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - timeout.exe (PID: 3384 cmdline: timeout /t 6 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Vidar

```
{
  "C2 url": "https://t.me/asifrazatg",
  "Botnet": "1148"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.244915415.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000002.231893309.000000000079A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000002.00000002.245065608.00000000006E7000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000003.232045586.00000000004BC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: file.exe PID: 5896	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.file.exe.526a20.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.file.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
2.2.file.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.3.file.exe.526a20.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.file.exe.7fb280.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking



C2 URLs / IPs found in malware configuration

System Summary



Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection



Self deletion via cmd or bat file

HIPS / PFW / Operating System Protection Evasion



Copyright Joe Security LLC 2022

Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Vidar stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Found many strings related to Crypto-Wallets (likely being stolen)

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

Remote Access Functionality

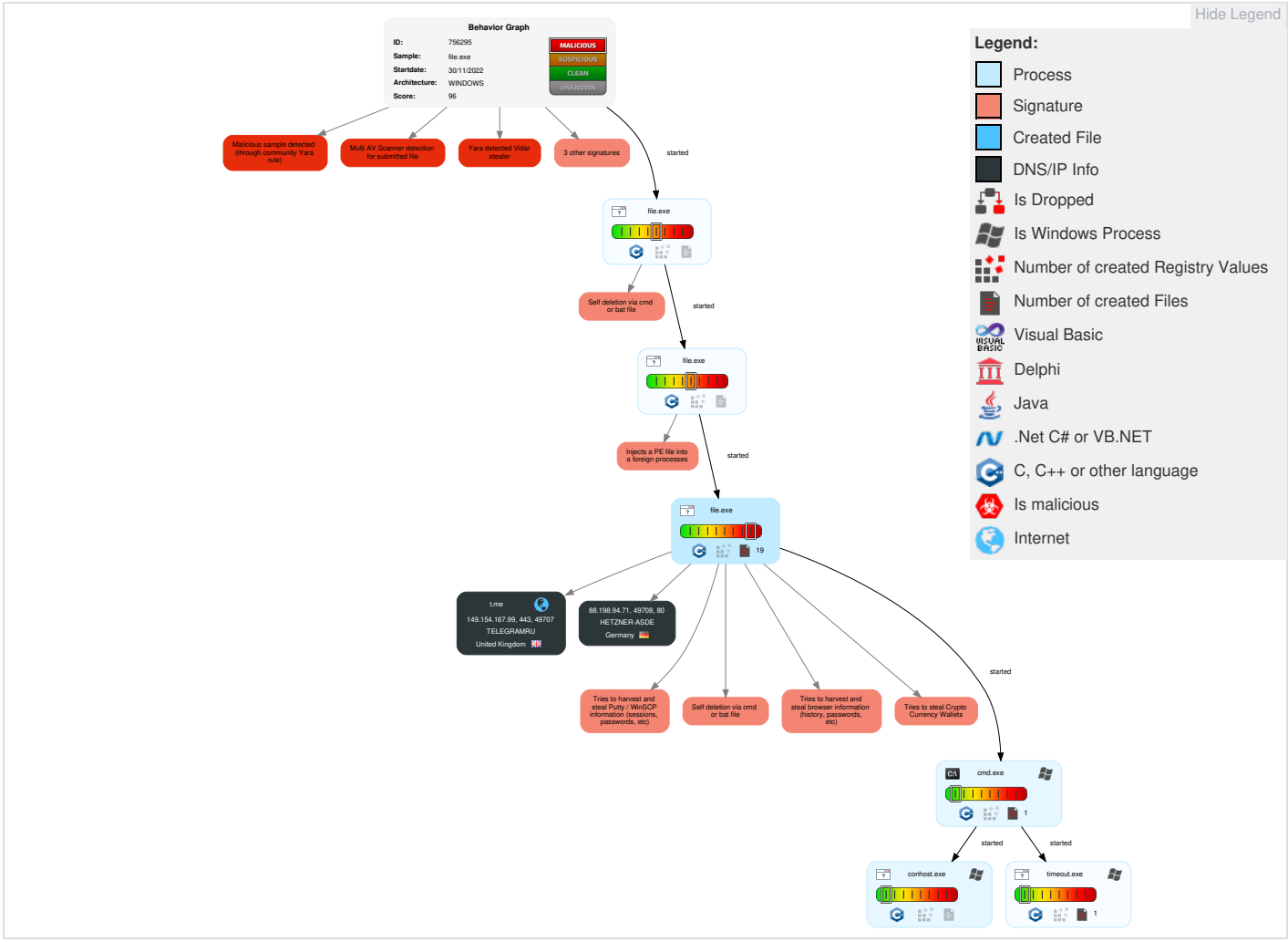


Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 1 1 Process Injection	1 Virtualization/Sandbox Evasion	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Screen Capture	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Credentials in Registry	2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	3 Data from Local System	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	4 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	5 4 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	32%	ReversingLabs	Win32.Infostealer.Bandra	
file.exe	37%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.file.exe.526a20.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.7fb280.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

URLs

Source	Detection	Scanner	Label	Link
http://88.198.94.71:80/233910279258.zipd87633a38bb03555514232-d06ed635-68f6-4e9a-955c-90ce-806e6f6e6	0%	Avira URL Cloud	safe	
http://116.202.6.206:80	3%	Virustotal		Browse
http://88.198.94.71/1148	4%	Virustotal		Browse
http://88.198.94.71/	1%	Virustotal		Browse
http://88.198.94.71:80/233910279258.zip	0%	Avira URL Cloud	safe	
http://88.198.94.71:80/233910279258.zip8C	0%	Avira URL Cloud	safe	
http://88.198.94.71/233910279258.zip	0%	Avira URL Cloud	safe	
http://88.198.94.71/	0%	Avira URL Cloud	safe	
http://116.202.6.206:80	0%	Avira URL Cloud	safe	
http://88.198.94.71/1148	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t.me	149.154.167.99	true	false		high

Contacted URLs

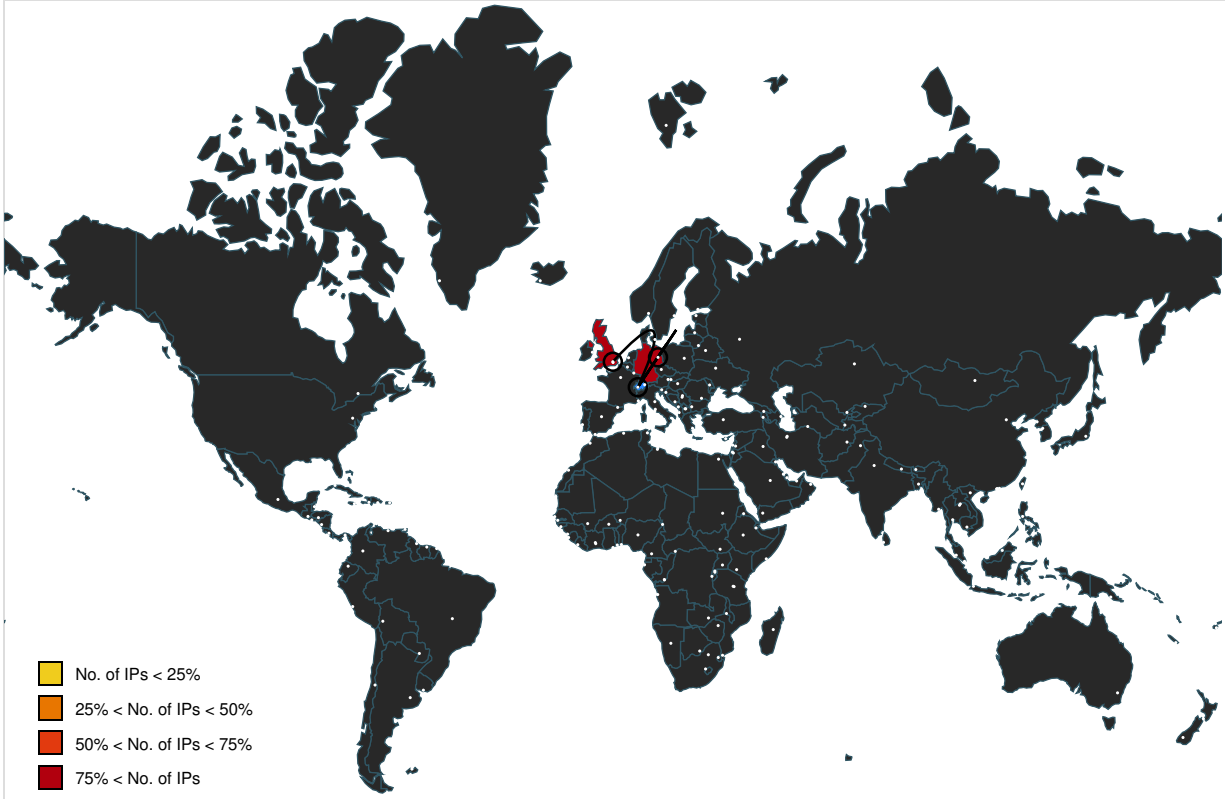
Name	Malicious	Antivirus Detection	Reputation
http://88.198.94.71/1148	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://t.me/asifrazatg	false		high
http://88.198.94.71/	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://88.198.94.71/233910279258.zip	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	583085593851864158761436 10.2.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	115657092571718131790630 97.2.dr, 583085593851864158761436 10.2.dr	false		high
http://https://duckduckgo.com/chrome_newtab	115657092571718131790630 97.2.dr, 583085593851864158761436 10.2.dr	false		high
http://https://t.me/	file.exe, 00000002.00000002.245065608.000000006E7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://88.198.94.71:80/233910279258.zipd87633a38bb03555514232-d06ed635-68f6-4e9a-955c-90ce-806e6f6e6	file.exe, 00000002.00000002.244899570.000000001AD000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://116.202.6.206:80	file.exe, file.exe, 00000002.00000002.244915415.000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	583085593851864158761436 10.2.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	115657092571718131790630 97.2.dr, 583085593851864158761436 10.2.dr	false		high
http://https://web.telegram.org	file.exe, 00000002.00000003.234690206.000000000764000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/asifrazatg&	file.exe, 00000002.00000002.245065608.000000006E7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/asifrazatghttps://steamcommunity.com/profiles/76561199439929669116.202.6.206:80p	file.exe, 00000002.00000002.244915415.000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	115657092571718131790630 97.2.dr, 583085593851864158761436 10.2.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	583085593851864158761436 10.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://88.198.94.71:80/233910279258.zip8C	file.exe, 00000002.00000002.245065608.000000006E7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://88.198.94.71:80/233910279258.zip	file.exe, 00000002.00000002.244899570.000000001AD000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	11565709257171813179063097.2.dr, 5830855938518641587614361 0.2.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	583085593851864158761436 10.2.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	11565709257171813179063097.2.dr, 5830855938518641587614361 0.2.dr	false		high
http://https://steamcommunity.com/profiles/76561199439929669	file.exe, file.exe, 00000002.00000002.244915415.000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.sqlite.org/copyright.html.	file.exe, 00000002.00000002.255872919.000000026C8C000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000002.00000002.257451716.0000000061ED3000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756295
Start date and time:	2022-11-30 00:09:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 34s

Copyright Joe Security LLC 2022

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.spyw.evad.winEXE@10/6@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.7% (good quality ratio 24.3%) • Quality average: 79.3% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

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\1026886203971244450577708

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 4, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.47881670276786453
Encrypted:	false
SSDEEP:	96:eVdU+bb3HDsX0ctSOaDN6tOVjN9DLjGQLBE3u:eVK+H3HDi9GN6IVj3XBBE3u
MD5:	C8A54C5A54BC6D813A12E47887D86821
SHA1:	98DDD99BBA14B47B75D4F8A53792221D162483FC
SHA-256:	00E175AD7C78A730A2754729174655A8686A663E878B88564F1D6164746FCF86
SHA-512:	BBC033381816DE6A86F34917F4A13486BE35DE0A4C4FD94EBF1306CDB106331C3417051B4269BA182D6410629513C92EB2700CCF6FDF4CF6415696B15C97ED5
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\11565709257171813179063097

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944
MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D5
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\48870274652683548820497570

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 4, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.47881670276786453
Encrypted:	false
SSDEEP:	96:eVdU+bb3HDsX0ctSOaDN6tOVjN9DLjGQLBE3u:eVK+H3HDi9GN6IVj3XBBE3u
MD5:	C8A54C5A54BC6D813A12E47887D86821
SHA1:	98DDD99BBA14B47B75D4F8A53792221D162483FC
SHA-256:	00E175AD7C78A730A2754729174655A8686A663E878B88564F1D6164746FCF86
SHA-512:	BBC033381816DE6A86F34917F4A13486BE35DE0A4C4FD94EBF1306CDB106331C3417051B4269BA182D6410629513C92EB2700CCF6FDF4CF6415696B15C97ED5
Malicious:	false

Preview:	SQLite format 3.....@ .....$.....)....[5..... ....

C:\ProgramData\58308559385186415876143610

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944
MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D5
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\82308976761520470245380715

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 10
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.4393511334109407
Encrypted:	false
SSDEEP:	24:TLqlj1czkwubXYFpFNYcw+6UwcYzHrSl:TyxcYwuLopFgU1YzLSl
MD5:	8C31C5487A97BBE73711C5E20600C1F6
SHA1:	D4D6B04226D8FFC894749B3963E7DB7068D6D773
SHA-256:	A1326E74262F4B37628F2E712EC077F499B113181A1E937E752D046E43F1689A
SHA-512:	394391350524B994504F4E748CCD5C3FA8EF980AED850A5A60F09250E8261AC8E300657CBB1DBF305729637BC0E1F043E57799E2A35C82EEA3825CE5C9E7051D
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\ProgramData\82668342394913559298137947

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.359412301232748
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	371200
MD5:	5367709f0a96713b5c9a518e13f306d6
SHA1:	244bdcc9a3548101cacc9c4f8912fb8631764b40
SHA256:	2cc0be582a350f1eafb6d3c6cc713393098a6936346a9070ba55abd346dfb090
SHA512:	e8ef72e92e7524f8529e4b9f0232550c07ced72971bff2072d1f81989a1f6174fca03100b540f777d87fd0048048af31bfd203c51d30ec584d490cb3424f84f8
SSDEEP:	6144:/Xd9qQwRToa3lQZCsPuugr+mJ35AfpJW+0sZZLBO+jJJM9KSlAo8hV:fdEVBoOlQnuuG+k3efD6sjLelAdb
TLSH:	8E84E041E718469EC97919F60431971F6F5458900FA082EB438FBE6A6B3368B87EFC43
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7?.yYI.yYI.yYI...I.yYI..]m.yYI..Zm.yYI..\m.yYI..Xm.yYI..Xm.yYI.yXI.yYIT.Pm.yYIT..I.yYIT.[m.yYIRich.yYI.....PE..L..

File Icon



Icon Hash:	00c1062769747441

Static PE Info

General

Entrypoint:	0x402851
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385E4DB [Tue Nov 29 10:54:19 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	6294a2f7da3a84900c7e91cad8ab870e

Entrypoint Preview

Instruction
call 00007FCC80F5E025h
jmp 00007FCC80F5D86Fh
retn 0000h
push ebp
mov ebp, esp
push 00000000h
call dword ptr [0040402Ch]
push dword ptr [ebp+08h]
call dword ptr [00404058h]
push C0000409h
call dword ptr [00404030h]

Instruction
push eax
call dword ptr [00404034h]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call dword ptr [00404038h]
test eax, eax
je 00007FCC80F5D9F7h
push 00000002h
pop ecx
int 29h
mov dword ptr [0044EFC8h], eax
mov dword ptr [0044EFC4h], ecx
mov dword ptr [0044EFC0h], edx
mov dword ptr [0044EFBCh], ebx
mov dword ptr [0044EFB8h], esi
mov dword ptr [0044EFB4h], edi
mov word ptr [0044EFE0h], ss
mov word ptr [0044EFD4h], cs
mov word ptr [0044EFB0h], ds
mov word ptr [0044EFACh], es
mov word ptr [0044EFA8h], fs
mov word ptr [0044EFA4h], gs
pushfd
pop dword ptr [0044EFD8h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [0044EFCCh], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [0044EFD0h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [0044EFDCh], eax
mov eax, dword ptr [ebp-00000324h]
mov dword ptr [0044EF18h], 00000001h

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x48fc	0xc8	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x50000	0xddd8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5e000	0x310	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x4300	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4240	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4000	0x11c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Copyright Joe Security LLC 2022

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2144	0x2200	False	0.5970818014705882	data	6.109737699299444	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x4000	0x10a6	0x1200	False	0.3993055555555556	data	4.440653872428405	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6000	0x497a8	0x49000	False	0.9481585776969178	data	7.658127773950707	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x50000	0xddd8	0xde00	False	0.09496410472972973	data	3.179746451017983	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	0x310	0x400	False	0.7275390625	data	5.550811047884393	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x500f0	0xda28	Device independent bitmap graphic, 105 x 256 x 32, image size 53760, resolution 25259 x 25259 px/m	Russian	Russia
RT_GROUP_ICON	0x5db18	0x14	data	Russian	Russia
RT_VERSION	0x5db30	0x2a8	data		

Imports

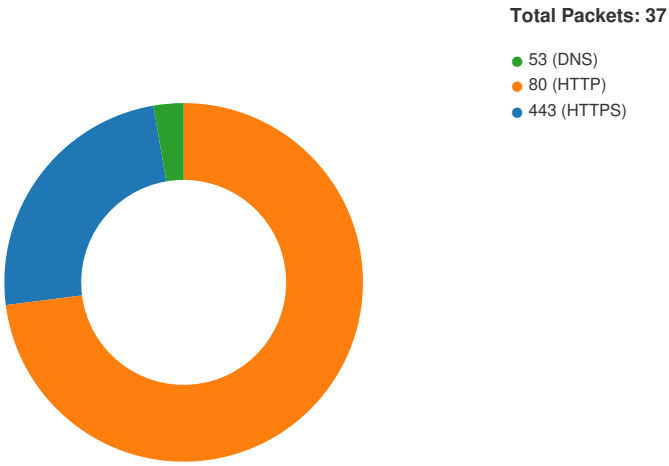
DLL	Import
KERNEL32.dll	GetModuleFileNameA, WriteProcessMemory, ResumeThread, GetModuleHandleA, GetThreadContext, GetProcAddress, ExitProcess, ReadProcessMemory, CreateProcessA, SetThreadContext, IsDebuggerPresent, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, GetStartupInfoW, GetModuleHandleW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, UnhandledExceptionFilter
MSVCP140.dll	?_Xlength_error@std@@YAXPBD@Z
VCRUNTIME140.dll	_except_handler4_common, memset, __current_exception_context, memcpy, _CxxThrowException, __std_exception_copy, __std_exception_destroy, __CxxFrameHandler3, __current_exception, memmove
api-ms-win-crt-runtime-l1-1-0.dll	_crt_atexit, _cexit, _seh_filter_exe, _set_app_type, _register_onexit_function, _initterm, _initterm_e, _exit, exit, _c_exit, _register_thread_local_exe_atexit_callback, _initialize_narrow_environment, _configure_narrow_argv, _get_narrow_winmain_command_line, terminate, _controlfp_s, _initialize_onexit_table, _invalid_parameter_noinfo_noreturn
api-ms-win-crt-stdio-l1-1-0.dll	_set_fmode, __p__commode
api-ms-win-crt-utility-l1-1-0.dll	rand, srand
api-ms-win-crt-heap-l1-1-0.dll	_callnewh, malloc, free, _set_new_mode
api-ms-win-crt-math-l1-1-0.dll	__setusermatherr
api-ms-win-crt-locale-l1-1-0.dll	_configthreadlocale

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:10:03.696094990 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:03.696155071 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:03.696418047 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:03.747873068 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:03.747900009 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:03.825840950 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:03.825999022 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:04.305008888 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:04.305059910 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.305671930 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.310623884 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:04.318892956 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:04.318938017 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.355186939 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.355230093 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.355340004 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.355359077 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.355654955 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:04.483719110 CET	49707	443	192.168.2.7	149.154.167.99
Nov 30, 2022 00:10:04.483772993 CET	443	49707	149.154.167.99	192.168.2.7
Nov 30, 2022 00:10:04.509978056 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.548715115 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.548928022 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.549756050 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.589503050 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.694690943 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.694907904 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.722865105 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.761621952 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762178898 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762217045 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762237072 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762262106 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762298107 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762319088 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762325048 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.762351036 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762366056 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.762372971 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762396097 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.762401104 CET	80	49708	88.198.94.71	192.168.2.7

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:10:04.762422085 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.762438059 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.762460947 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.800975084 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801017046 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801089048 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801126957 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801203966 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801224947 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801260948 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801296949 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801311016 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801341057 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801362991 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801369905 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801384926 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801392078 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801428080 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801451921 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801453114 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801472902 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801482916 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801496029 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801517010 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801517963 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801541090 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801574945 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801589966 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801599979 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801621914 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801631927 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801645041 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801661015 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801666975 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.801701069 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.801937103 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.840192080 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840213060 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840240002 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840260983 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840298891 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840318918 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840343952 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840363979 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840401888 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840419054 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.840430021 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840451002 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840475082 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.840476036 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840497017 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840523005 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840543985 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840563059 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840573072 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.840585947 CET	49708	80	192.168.2.7	88.198.94.71
Nov 30, 2022 00:10:04.840595961 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840616941 CET	80	49708	88.198.94.71	192.168.2.7
Nov 30, 2022 00:10:04.840636969 CET	80	49708	88.198.94.71	192.168.2.7

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:10:03.656122923 CET	56588	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:10:03.672709942 CET	53	56588	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:10:03.656122923 CET	192.168.2.7	8.8.8.8	0x2a4	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false

DNS Answers

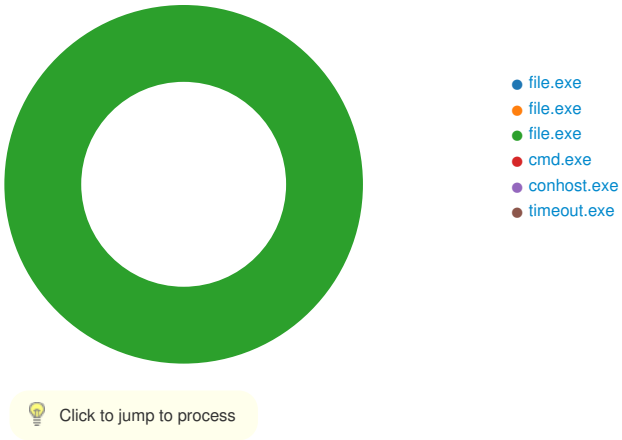
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:10:03.672709942 CET	8.8.8.8	192.168.2.7	0x2a4	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- t.me
- 88.198.94.71

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 5884, Parent PID: 3320

General

Target ID:	0
Start time:	00:10:02
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0xe80000
File size:	371200 bytes
MD5 hash:	5367709F0A96713B5C9A518E13F306D6
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: 00000000.00000002.231893309.000000000079A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: file.exe PID: **5924**, Parent PID: **5884**

General

Target ID:	1
Start time:	00:10:03
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0xe80000
File size:	371200 bytes
MD5 hash:	5367709F0A96713B5C9A518E13F306D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000003.232045586.00000000004BC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: file.exe PID: **5896**, Parent PID: **5924**

General

Target ID:	2
Start time:	00:10:03
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0xe80000
File size:	371200 bytes
MD5 hash:	5367709F0A96713B5C9A518E13F306D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000002.00000002.244915415.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.245065608.00000000006E7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **5984**, Parent PID: **5896**

General

Target ID:	3

Start time:	00:10:09
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\Desktop\file.exe" & exit
Imagebase:	0xa60000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4656**, Parent PID: **5984**

General

Target ID:	4
Start time:	00:10:09
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: **3384**, Parent PID: **5984**

General

Target ID:	5
Start time:	00:10:09
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 6
Imagebase:	0xdb0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly