ID: 736713
Sample Name: file.exe
Cookbook: default.jbs
Time: 06:42:23
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

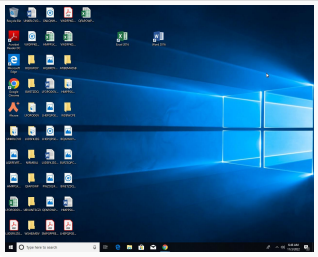
Windows Analysis Report

file.exe

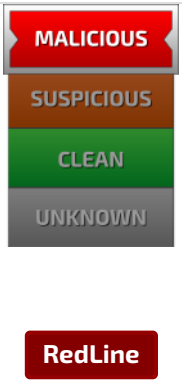
Overview

General Information

Sample Name:	file.exe
Analysis ID:	736713
MD5:	67756a08917974.
SHA1:	4cbd4192bb33d1..
SHA256:	ba3a496df23cb2..
Tags:	exe
Infos:	



Detection



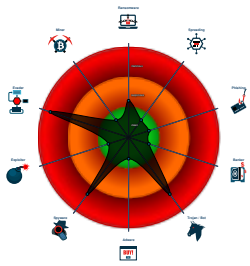
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Tries to steal Crypto Currency Walle…
- Machine Learning detection for sam…
- Queries sensitive video device infor…
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…
- Found many strings related to Crypt…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5600 cmdline: C:\Users\user\Desktop\file.exe MD5: 67756A08917974F3E77B7B2E2BCCF264)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": "193.106.191.25:47242",
  "Bot Id": "mix",
  "Authorization Header": "5469d87831a100553f2f10d3aadec8bb"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.305323613.0000000000860000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.305323613.0000000000860000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000002.305740549.0000000000959000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0xb80:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.306398043.00000000022F6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.243234104.00000000009CE000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.400000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.file.exe.400000.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e4b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x1300:$s3: 83 EC 38 53 B0 D2 88 44 24 2B 88 44 24 2F B0 10 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B($B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.
0.2.file.exe.2820ee8.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.file.exe.2820ee8.4.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x28338:$pat14: , CommandLine: • 0x1ca87:$v2_1: ListOfProcesses • 0x1c255:$v4_3: base64str • 0x1c222:$v4_4: stringKey • 0x1c25f:$v4_5: BytesToStringConverted • 0x1c24a:$v4_6: FromBase64 • 0x1c73b:$v4_8: procName
0.2.file.exe.860e67.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 27 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 193.106.191.25

Timestamp:	192.168.2.3193.106.191.2549699472422850027 11/03/22-06:43:26.443077
SID:	2850027
Source Port:	49699
Destination Port:	47242
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 193.106.191.25

Timestamp:	192.168.2.3193.106.191.2549699472422850286 11/03/22-06:43:32.777356
SID:	2850286
Source Port:	49699
Destination Port:	47242
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 193.106.191.25 - Destination IP: 192.168.2.3	
Timestamp:	193.106.191.25192.168.2.347242496992850353 11/03/22-06:43:29.233425
SID:	2850353
Source Port:	47242
Destination Port:	49699
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Machine Learning detection for sample

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 (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

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

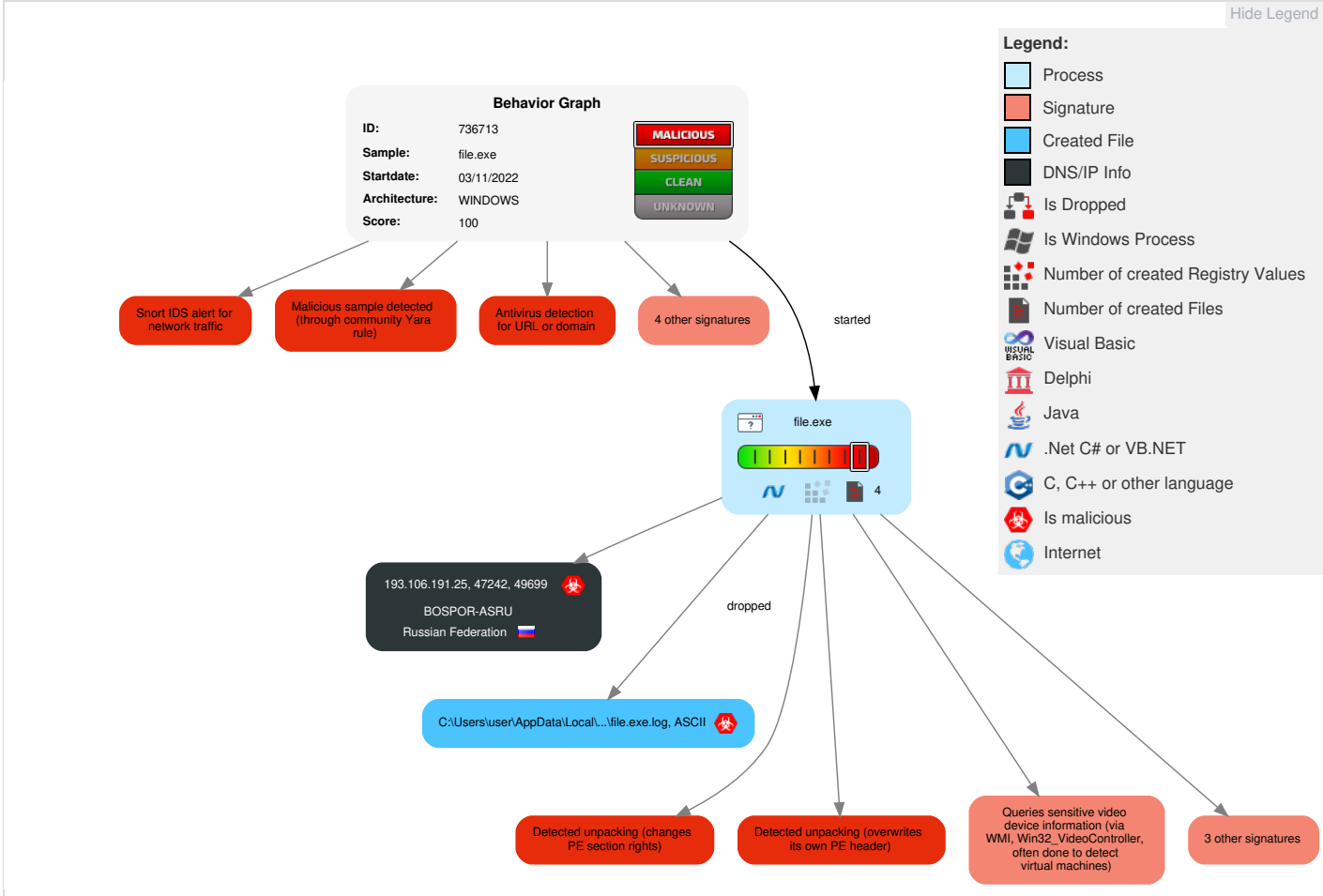
Remote Access Functionality

Yara detected RedLine 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 2 1 Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	2 6 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Native API	Logon Script (Windows)	Logon Script (Windows)	2 3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	3 Data from Local System	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 Application Window 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	2 Software Packing	Cached Domain Credentials	1 3 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

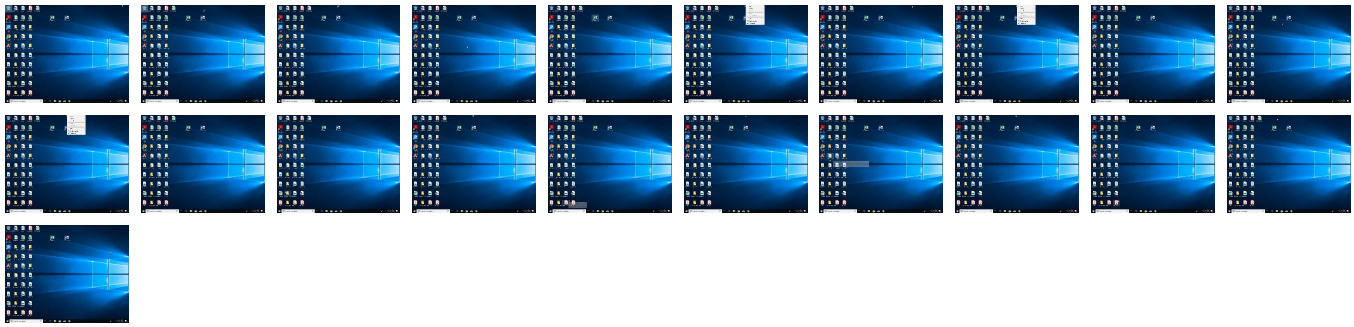
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://www.w3.o	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1	0%	URL Reputation	safe	
193.106.191.25:47242	2%	Virustotal		Browse
193.106.191.25:47242	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
193.106.191.25:47242	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	file.exe, 00000000.00000002.307819441.000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	file.exe, 00000000.00000002.307819441.000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	file.exe, 00000000.00000002.318900508.00000000003A35000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.311190508.0000000002BFB000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318080589.000000000393F000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319643786.0000000003B30000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319251031.0000000003AB2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318633797.0000000039D4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319732185.0000000003B4D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319019701.0000000003A52000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.320023211.0000000003BC7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318003971.0000000003922000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318530796.00000000039B7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319896306.00000003BAA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319381075.0000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	file.exe, 00000000.00000002.319381075.00000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.306398043.00000000022F6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.243234104.00000000009CE000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.307296597.0000000002820000.00000004.08000000.00040000.00000000.sdmp, file.exe, 00000000.00000002.320137797.0000000005220000.00000004.08000000.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	file.exe, 00000000.00000002.319381075.00000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	file.exe, 00000000.00000002.318900508.00000000003A35000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.311190508.0000000002BFB000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318080589.00000000000393F000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319643786.0000000003B30000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319251031.0000000003AB2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318633797.0000000000039D4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319732185.0000000003B4D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319019701.0000000003A52000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.320023211.0000000003BC7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318003971.0000000003922000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318530796.00000000039B7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319896306.00000000003BAA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319381075.0000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high

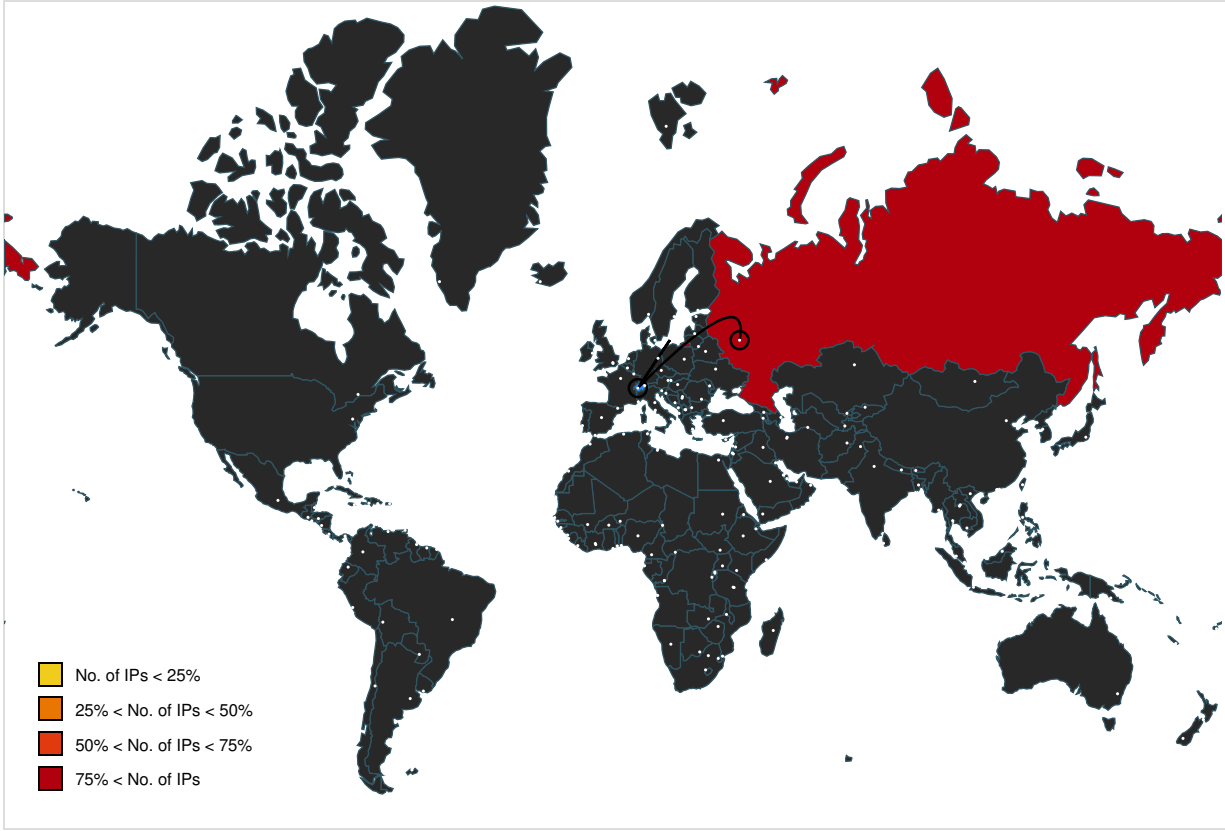
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	file.exe, 00000000.00000002.318900508.00000003A35000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.311190508.0000000002BFB000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318080589.000000000393F000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319643786.0000000003B30000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319251031.0000000003AB2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318633797.000000000039D4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319732185.0000000003B4D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319019701.0000000003A52000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.320023211.0000000003BC7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318003971.0000000003922000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318530796.00000000039B7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319896306.00000003BAA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319381075.0000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.w3.o	file.exe, 00000000.00000002.308423894.00000002A2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/fault	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possessproperty	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/RegisterResponse	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Cancel	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	file.exe, 00000000.00000002.307819441.00000002942000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	file.exe, 00000000.00000002.318900508.00000000003A35000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.311190508.0000000002BFB000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318080589.000000000393F000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319643786.0000000003B30000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319251031.0000000003AB2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318633797.0000000039D4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319732185.0000000003B4D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319019701.0000000003A52000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.320023211.0000000003BC7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318003971.0000000003922000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318530796.00000000039B7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319896306.00000003BAA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319381075.0000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/tlsnego#TLS_Wrap	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2002/12/policy	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/dk	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Issue	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	file.exe, 00000000.00000002.318900508.0000000003A35000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.311190508.0000000002BFB000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318080589.00000000393F000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319643786.0000000003B30000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319251031.0000000003AB2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318633797.00000000039D4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319732185.0000000003B4D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319019701.0000000003A52000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.320023211.0000000003BC7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318003971.0000000003922000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.318530796.00000000039B7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319896306.0000000003BAA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.319381075.0000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/Issue	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Commit	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContext	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Issue	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT	file.exe, 00000000.00000002.307819441.00000000002942000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1	file.exe, 00000000.00000002.307685962.000000028E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	file.exe, 00000000.00000002.319381075.0000000003ACF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.309635503.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.106.191.25	unknown	Russian Federation		42238	BOSPOR-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736713
Start date and time:	2022-11-03 06:42:23 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 12s
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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 40.5% (good quality ratio 38.8%) • Quality average: 84.9% • Quality standard deviation: 24.9%

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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:44:23	API Interceptor	65x Sleep call for process: file.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHK5HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHK1HG1qH5HZHDJH6:Pq5qXdq7qLqdqUqzcGYqhQnoPtIxHbq0
MD5:	7D9A4122E2F2920B18399BEE36A6987C
SHA1:	201FAC07241D6DA7885E81E3980C62F994DB58CC
SHA-256:	024B1A66ADDF6A7829F618EA7BA9CCB626646E4D116FB362174766E218EC62CC

SHA-512:	6DB9776956B2959B98B63EB69C7B04E63CCFDBD4E62B6FC75A05AA385F73D9BEF63CF3A67C021DA2CBF7C06AE2CCC6A111FCFE09E7D3BD8D49A93CB47C7E680F
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.463503080951417
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	357888
MD5:	67756a08917974f3e77b7b2e2bccf264
SHA1:	4cbd4192bb33d1d6760214ee2758e8a2be7fc847
SHA256:	ba3a496df23cb27c37b3765e630c4b637f3b82166621589e953906b1ca29b049
SHA512:	5c4b27efb5375644203d04c2ba9d49cc4bf0c273ec34f208bef4adf9dfa19acc61788fbea40032a1f7cdba68c16b3493465dc962fdc3e3ad1855e404772bbb0d
SSDEEP:	6144:gUaDQpMwaLww3ZKP2lA0/lhoi1uT+873/6appA8F9P9pysfnF:gUOQfasw3lOJP+x7CappAA9P9p7fF
TLSH:	1B74F1223591C072D66A12348C15CAB56FAFB87409359BAB3FC91ABD4F342D2DE3531B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.^.".^.".^.".@...C.".@.....".y.Y.Y.".^.#...".@...l.".@..._.".@..._.".Rich^."........PE..L....Q.a.....N.....

File Icon

Icon Hash:	a0b0b0b4e8c6ce4a

Static PE Info

General

Entrypoint:	0x4094f6
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:	0x618851BF [Sun Nov 7 22:22:55 2021 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:	8fb85d04360d27123c3a8e1c2ffb7f7e

Entrypoint Preview

Instruction
call 00007F5C5CAAB632h
jmp 00007F5C5CAA361Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
test eax, eax
je 00007F5C5CAA37B4h
sub eax, 08h
cmp dword ptr [eax], 0000DDDDh
jne 00007F5C5CAA37A9h
push eax
call 00007F5C5CAA2C72h
pop ecx
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007F5C5CAA3805h
call 00007F5C5CAA8110h
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [00453E88h]
je 00007F5C5CAA37B4h
mov ecx, dword ptr [00453DA0h]
test dword ptr [eax+70h], ecx
jne 00007F5C5CAA37A9h
call 00007F5C5CAA49B1h
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [00453CA8h]
je 00007F5C5CAA37B8h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [00453DA0h]
test dword ptr [eax+70h], ecx
jne 00007F5C5CAA37AAh
call 00007F5C5CAAB869h
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007F5C5CAA37B6h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007F5C5CAA37ACh
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi

Instruction
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 14h
mov eax, dword ptr [004533ACh]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push esi
xor ebx, ebx

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [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	0x1e7e4	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1ae000	0x4310	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1280	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4348	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x220	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1e44a	0x1e600	False	0.5126189557613169	data	6.390774871628584	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x20000	0x18d984	0x34800	False	0.9630022321428572	data	7.9198667435711165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1ae000	0x4310	0x4400	False	0.5094784007352942	data	4.749144797854934	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RIWEZOZAC	0x1b1700	0x55f	ASCII text, with very long lines (1375), with no line terminators	Romanian	Romania
RT_ICON	0x1ae330	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Romanian	Romania
RT_ICON	0x1aebd8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Romanian	Romania

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1af2a0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Romanian	Romania
RT_ICON	0x1af808	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Romanian	Romania
RT_ICON	0x1b08b0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Romanian	Romania
RT_ICON	0x1b1238	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Romanian	Romania
RT_STRING	0x1b1e08	0xb6	data	Romanian	Romania
RT_STRING	0x1b1ec0	0x2ae	data	Romanian	Romania
RT_STRING	0x1b2170	0x19c	data	Romanian	Romania
RT_ACCELERATOR	0x1b1c60	0x58	data	Romanian	Romania
RT_GROUP_ICON	0x1b16a0	0x5a	data	Romanian	Romania
RT_VERSION	0x1b1cb8	0x14c	Intel 80386 COFF executable, no relocation info, not stripped, 52 sections, symbol offset=0x5f0053, 4522070 symbols, optional header size 82, created Sat Mar 7 05:34:56 1970		

Imports

DLL	Import
KERNEL32.dll	LocalSize, InterlockedExchange, GetTickCount, CopyFileExA, GetConsoleAliasExesLengthW, EnumSystemCodePagesA, TlsGetValue, MoveFileWithProgressA, VerifyVersionInfoW, LocalUnlock, DebugBreak, GlobalGetAtomNameA, MapViewOfFileEx, GetWindowsDirectoryA, GetModuleHandleA, lstrlenW, GlobalDeleteAtom, SizeofResource, WriteConsoleInputA, CopyFileW, SetWaitableTimer, GetVersionExA, FindResourceW, OpenEventA, SearchPathA, GetThreadPriority, CallNamedPipeA, GetProcAddress, GlobalAlloc, SetFileTime, GetConsoleAliasesLengthA, GetComputerNameA, GetSystemWindowsDirectoryA, GetMailslotInfo, GetTapeParameters, OpenJobObjectW, GetPrivateProfileIntA, ReadConsoleInputW, _lread, LockFile, GetPrivateProfileStructW, GetDiskFreeSpaceExW, DefineDosDeviceW, GetACP, SetProcessAffinityMask, GlobalFindAtomW, InterlockedDecrement, VerifyVersionInfoA, CreateActCtxW, FindNextVolumeA, GetComputerNameW, CancelDeviceWakeupRequest, EnumCalendarInfoA, InterlockedCompareExchange, GetPrivateProfileStructA, EnumCalendarInfoW, EnterCriticalSection, InterlockedIncrement, GetNamedPipeHandleStateW, AreFileApisANSI, LoadLibraryA, SetLastError, WriteConsoleW, GetVolumeInformationA, OpenFileMappingA, LoadLibraryW, Sleep, InitializeCriticalSection, DeleteCriticalSection, LeaveCriticalSection, RtlUnwind, RaiseException, GetLastError, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapReAlloc, HeapAlloc, MoveFileA, DeleteFileA, GetStartupInfoW, LCMapStringA, WideCharToMultiByte, MultiByteToWideChar, LCMapStringW, GetCPInfo, GetModuleHandleW, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, HeapCreate, VirtualFree, VirtualAlloc, HeapSize, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, SetHandleCount, GetFileType, GetStartupInfoA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, GetStringTypeW, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, InitializeCriticalSectionAndSpinCount, SetFilePointer, GetConsoleCP, GetConsoleMode, GetLocaleInfoW, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, CloseHandle, CreateFileA
GDI32.dll	GetCharWidthA
ADVAPI32.dll	SetThreadToken

Possible Origin

Language of compilation system	Country where language is spoken	Map
Romanian	Romania	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.106.191.254969472422850027 11/03/22-06:43:26.443077	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49699	47242	192.168.2.3	193.106.191.25
192.168.2.3193.106.191.254969472422850286 11/03/22-06:43:32.777356	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49699	47242	192.168.2.3	193.106.191.25

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
193.106.191.25192.168.2.34724249699285035311/03/22-06:43:29.233425	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	47242	49699	193.106.191.25	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 06:43:26.097611904 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:26.155242920 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:26.155344963 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:26.443077087 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:26.500793934 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:26.546669960 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:29.175399065 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:29.233424902 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:29.287863970 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:32.777355909 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:32.846524000 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:32.846554041 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:32.846565962 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:32.846577883 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:32.846591949 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:32.846884012 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:43.922715902 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:43.980326891 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:43.980422974 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:43.980453968 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:43.982151985 CET	47242	49699	193.106.191.25	192.168.2.3
Nov 3, 2022 06:43:44.022700071 CET	49699	47242	192.168.2.3	193.106.191.25
Nov 3, 2022 06:43:44.028961897 CET	49699	47242	192.168.2.3	193.106.191.25

Statistics

No statistics

System Behavior

Analysis Process: file.exe PID: 5600, Parent PID: 3452

General

Target ID:	0
Start time:	06:44:01
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	357888 bytes
MD5 hash:	67756A08917974F3E77B7B2E2BCCF264
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.305323613.0000000000860000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.305323613.0000000000860000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.305740549.0000000000959000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.306398043.00000000022F6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.243234104.00000000009CE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.305087718.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.305087718.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.307296597.0000000002820000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.307296597.0000000002820000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.307819441.0000000002942000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.242826685.00000000008D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000003.242826685.00000000008D0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.320137797.0000000005220000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.320137797.0000000005220000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.312027149.0000000002C80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	6D30CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D30CF06	unknown
C:\Users\user\AppData\Local\Microsoft\Wind?ws	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C15BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D61C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	0	2291	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D61C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D2E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D2E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D2ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D2E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D2E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	6C151B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	5	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	21	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	24	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	37	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C151B4F	ReadFile

Disassembly

No disassembly