

JoeSandbox Cloud BASIC



ID: 756296

Sample Name: file.exe

Cookbook: default.jbs

Time: 00:10:11

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: RedLine	4
Yara Signatures	4
PCAP (Network Traffic)	4
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	6
Networking	6
System Summary	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	15
Public IPs	16
General Information	16
Warnings	17
Simulations	17
Behavior and APIs	17
Joe Sandbox View / Context	17
IPs	17
Domains	17
ASNs	17
JA3 Fingerprints	17
Dropped Files	17
Created / dropped Files	17
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log	17
Static File Info	18
General	18
File Icon	18
Static PE Info	18
General	18
Entrypoint Preview	18
Data Directories	20
Sections	20
Imports	21
Network Behavior	21
Snort IDS Alerts	21
TCP Packets	21
Statistics	23
Behavior	23
System Behavior	24
Analysis Process: file.exePID: 5316, Parent PID: 3452	24
General	24
File Activities	24
Analysis Process: conhost.exePID: 5332, Parent PID: 5316	24
General	24
Analysis Process: vbc.exePID: 5384, Parent PID: 5316	24
General	24

File Activities	25
File Created	25
File Written	25
File Read	25
Disassembly	27

Windows Analysis Report

file.exe

Overview

General Information

Sample Name:

file.exe

Analysis ID:

756296

MD5:

b285997d1fb1ed..

SHA1:

64fe09e86b2e6d..

SHA256:

8edce063ac9af6...

Tags:

exe

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

RedLine

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Yara detected RedLine Stealer

Malicious sample detected (through...

Snort IDS alert for network traffic

Writes to foreign memory regions

Tries to steal Crypto Currency Walle...

Allocates memory in foreign process...

Injects a PE file into a foreign proce...

Queries sensitive video device infor...

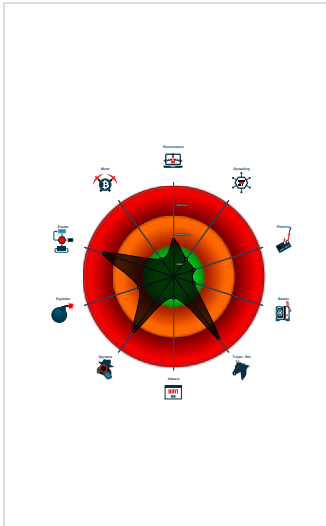
Contains functionality to inject code...

Queries sensitive disk information (v...

C2 URLs / IPs found in malware con...

Tries to harvest and steal browser in...

Classification



Process Tree

System is w10x64

file.exe

(PID: 5316 cmdline: C:\Users\user\Desktop\file.exe MD5: B285997D1FB1ED7FF9129E4E9566C2E5)

conhost.exe

(PID: 5332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

vbc.exe

(PID: 5384 cmdline: C:\Windows\Microsoft.NET\Framework\4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)

cleanup

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "172.86.120.146:2819"
  ],
  "Bot Id": "1kMixWorldTest",
  "Authorization Header": "7158f67354faaa79bd6ac126ef4cf20e"
}
```

Yara Signatures

PCAP (Network Traffic)				
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps				
Source	Rule	Description	Author	Strings
00000000.00000003.263012533.00000000010B2000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.356537948.0000000006AB2000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.356537948.0000000006AB2000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.263412439.00000000004A2000.0000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: file.exe PID: 5316	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
0.3.file.exe.10b0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.file.exe.10b0000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	0x2104c:\$pat14: , CommandLine: 0x18d58:\$v2_1: ListOfProcesses 0x18aec:\$v4_3: base64str 0x19b7f:\$v4_4: stringKey 0x16708:\$v4_5: BytesToStringConverted 0x15770:\$v4_6: FromBase64 0x16edc:\$v4_8: procName 0x1725f:\$v5_1: DownloadAndExecuteUpdate 0x189fc:\$v5_2: ITaskProcessor 0x1724d:\$v5_3: CommandLineUpdate 0x1723e:\$v5_4: DownloadUpdate 0x178f0:\$v5_5: FileScanning 0x16a77:\$v5_7: RecordHeaderField 0x16496:\$v5_9: BCrypt_Key_Lengths_Struct
0.2.file.exe.4a17a0.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.file.exe.4a17a0.1.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	0x1f44c:\$pat14: , CommandLine: 0x17158:\$v2_1: ListOfProcesses 0x16eec:\$v4_3: base64str 0x17f7f:\$v4_4: stringKey 0x14b08:\$v4_5: BytesToStringConverted 0x13b70:\$v4_6: FromBase64 0x152dc:\$v4_8: procName 0x1565f:\$v5_1: DownloadAndExecuteUpdate 0x16dfc:\$v5_2: ITaskProcessor 0x1564d:\$v5_3: CommandLineUpdate 0x1563e:\$v5_4: DownloadUpdate 0x15cf0:\$v5_5: FileScanning 0x14e77:\$v5_7: RecordHeaderField 0x14896:\$v5_9: BCrypt_Key_Lengths_Struct
0.2.file.exe.3e0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures	
	No Sigma rule has matched

Snort Signatures	
ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 172.86.120.146	
Timestamp:	192.168.2.3172.86.120.1464968428192850286 11/30/22-00:11:55.241038
SID:	2850286
Source Port:	49684
Destination Port:	2819
Protocol:	TCP
Class type:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 172.86.120.146	
Timestamp:	192.168.2.3172.86.120.1464968428192850027 11/30/22-00:11:30.935107
SID:	2850027
Source Port:	49684
Destination Port:	2819
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 172.86.120.146 - Destination IP: 192.168.2.3	
Timestamp:	172.86.120.146192.168.2.32819496842850353 11/30/22-00:11:32.905229
SID:	2850353
Source Port:	2819
Destination Port:	49684
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Networking



Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary



Malicious sample detected (through community Yara rule)

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)

HIPS / PFW / Operating System Protection Evasion



Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Stealing of Sensitive Information



Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

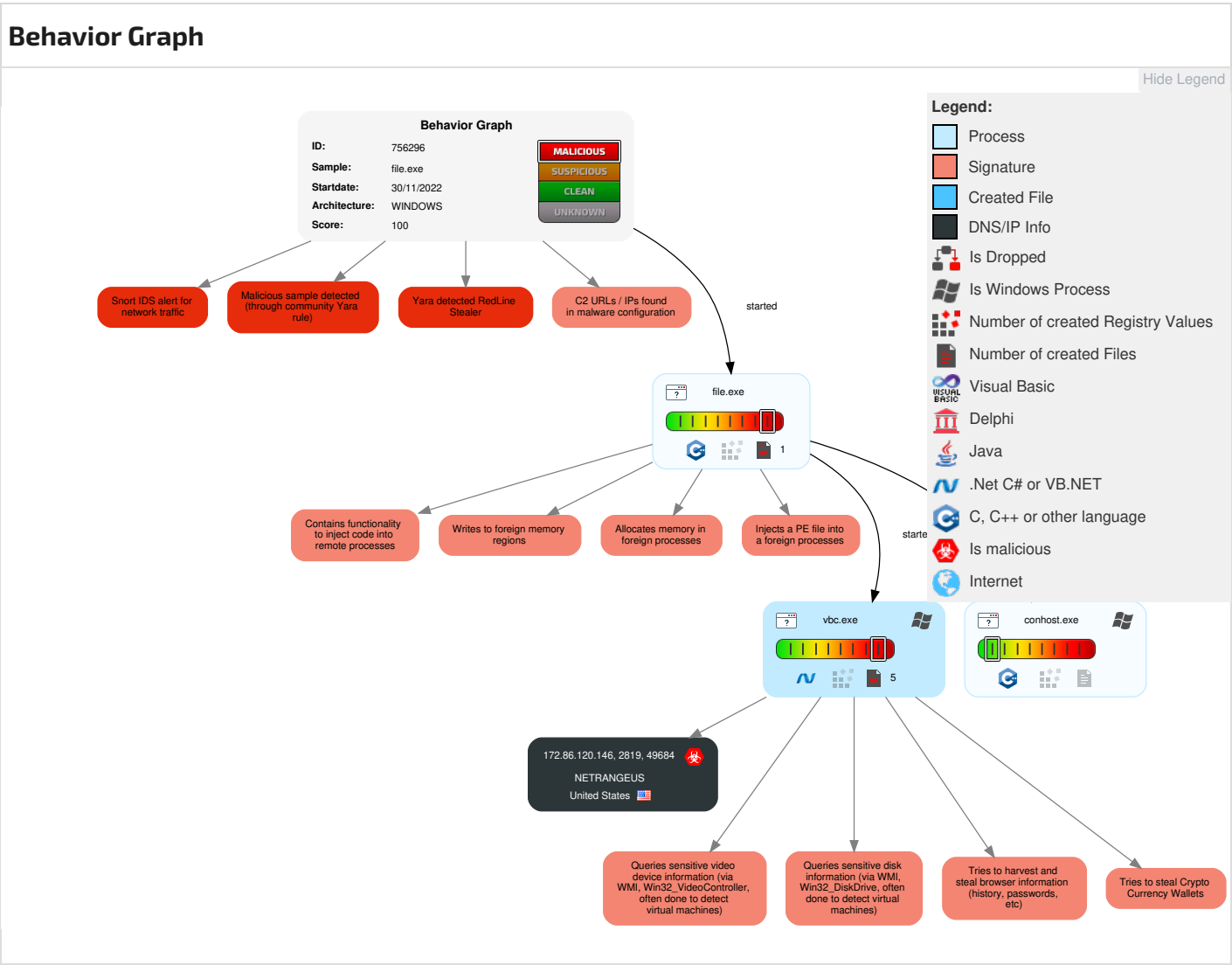
Remote Access Functionality



Yara detected RedLine Stealer

Mitre Att&ck Matrix

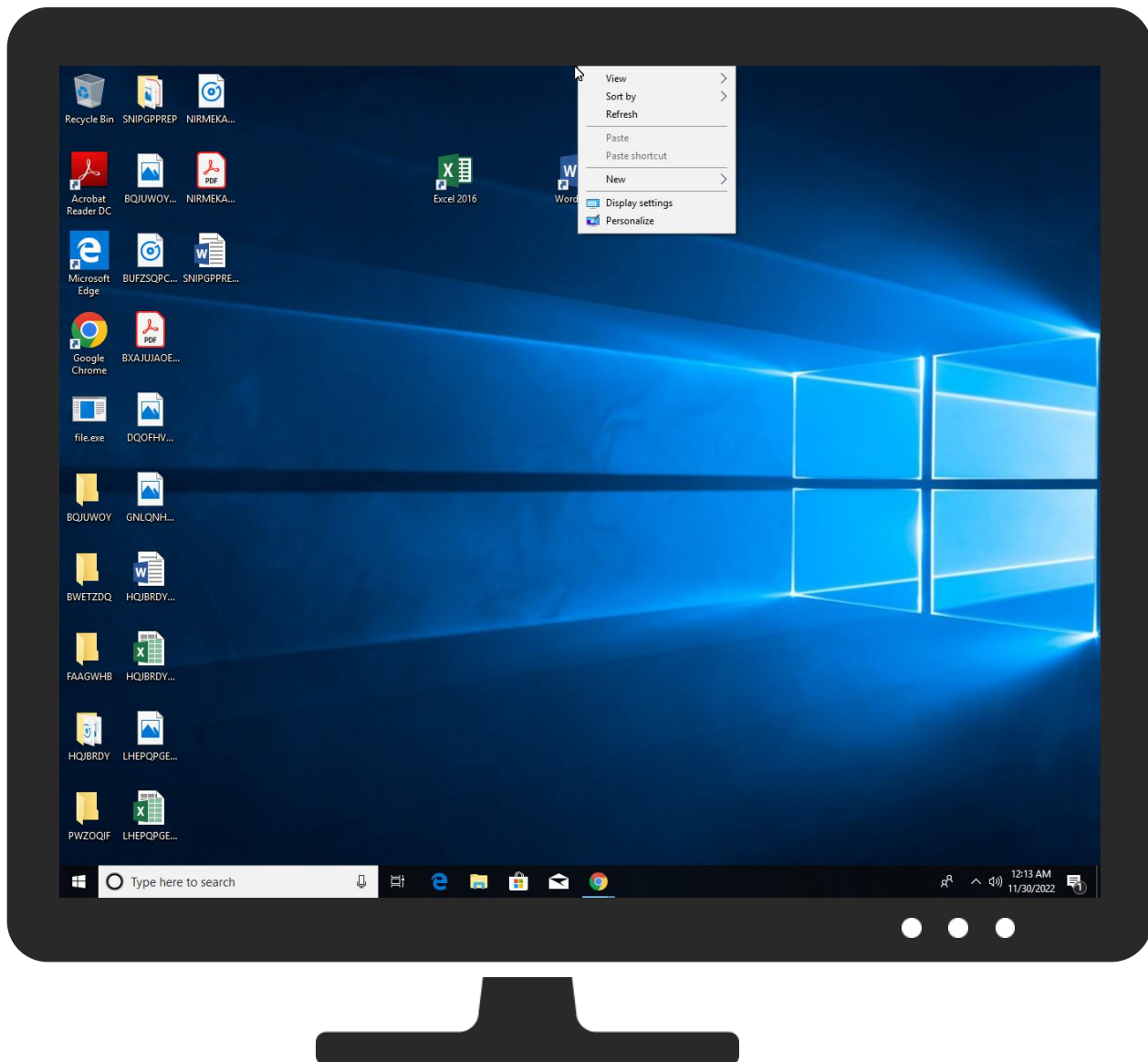
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 2 1 Windows Management Instrumentation	Path Interception	4 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 1 Process Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	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	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 1 1 Process Injection	NTDS	1 Application Window 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	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 2 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features



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

 No Antivirus matches

Dropped Files

 No Antivirus matches

Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23Response	0%	URL Reputation	safe	
http://ns.adoboshop/\$	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id4pe	1%	Virustotal		Browse
http://tempuri.org/Entity/Id4pe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

 No contacted domains info

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	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	vbc.exe, 00000002.00000002.362689753.00000007D26000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.358855894.0000000006CF1000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.357196581.0000000006B53000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.362080107.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.361557498.0000000007BCE000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.361472237.00000007BB1000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.362548163.0000000007D09000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.364377850.0000000007EC8000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.364566369.0000000007EE5000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363666444.0000000007E21000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.358245791.00000006C64000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.362239438.0000000007CA8000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363083426.0000000007D87000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.363208113.0000000007DA4000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363550422.0000000007E05000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://gcc.gnu.org/bugs/ :	file.exe	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	vbc.exe, 00000002.00000002.363208113.00000007DA4000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363550422.0000000007E05000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	vbc.exe, 00000002.00000002.357253699.00000006B60000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.355948732.0000000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.355948732.0000000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id21Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	- URL Reputation: safe - URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	- URL Reputation: safe - URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	- URL Reputation: safe - URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsdl/Prepare	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id7	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsdl/Aborted	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsdl/fault	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsdl	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adobeshop/\$	vbc.exe, 00000002.00000002.354699898.00000004E86000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Re new	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.355948732.0000000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	file.exe, file.exe, 00000000.00000003.263012533.000000010B2000.00000004.00001000.00020000.0.00000000.sdmp, file.exe, 00000000.00000002.263412439.00000000004A2000.00000004.00000001.01000000.00000003.sdmp, vbc.exe, 00000002.00000002.356537948.000000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/WSAT/2PC	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.357253699.0000000006B60000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	vbc.exe, 00000002.00000002.363208113.00000007DA4000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363550422.0000000007E05000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.357253699.0000000006B60000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.355948732.0000000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=cymas_sfp&command=	vbc.exe, 00000002.00000002.362689753.000000007D26000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.358855894.0000000006CF1000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.357196581.0000000006B53000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.362080107.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.361557498.0000000007BCE000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.361472237.000000007BB1000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.362548163.0000000007D09000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.364377850.0000000007EC8000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.364566369.0000000007EE5000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363666444.0000000007E21000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.358245791.000000006C64000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.362239438.0000000007CA8000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363083426.0000000007D87000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.363208113.0000000007DA4000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363550422.0000000007E05000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/soap/ReadOnly	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/soap/Replay	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/soap/Durable2PC	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/soap/Completion	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id16Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	- URL Reputation: safe - URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscor/CreateCoordinationContextResponse	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	- URL Reputation: safe - URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/soap/envelope/	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	vbc.exe, 00000002.00000002.362689753.00000007D26000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.358855894.0000000006CF1000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.357196581.0000000006B53000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.362080107.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000000.2.00000002.361557498.0000000007BCE000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.361472237.00000007BB1000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.361472237.00000007BB1000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.362548163.0000000007D09000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.364377850.0000000007EC8000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.364566369.0000000007EE5000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000000.2.00000002.363666444.0000000007E21000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.358245791.00000006C64000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.362239438.0000000007CA8000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.363083426.0000000007D87000.00000004.00000800.00020000.00000000.0.sdmp, vbc.exe, 00000002.00000002.363208113.0000000007DA4000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000000.2.00000002.363550422.0000000007E05000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23Response	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.355948732.0000000006A21000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.357253699.0000000006B60000.00000004.00000800.00020000.00000000.0.sdmp	false	URL Reputation: safe	unknown
http://tempuri.org/Entity/Id4pe	vbc.exe, 00000002.00000002.355948732.00000006A21000.00000004.00000800.00020000.00000000.sdmp	false	1%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscor	vbc.exe, 00000002.00000002.356537948.00000006AB2000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.86.120.146	unknown	United States		17139	NETRANGEUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756296
Start date and time:	2022-11-30 00:10:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 16s
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:	13
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@4/1@0/1
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 7.2% (good quality ratio 4.1%) - Quality average: 29.7% - Quality standard deviation: 28.1%

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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes were analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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
00:11:51	API Interceptor	28x Sleep call for process: vbc.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\vbc.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MxHKXeHKIEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHlmHKAHKx1V:iqXeqm00YqhQnouOqLqdqNq2qzcGtlxo
MD5:	AA480F97CE07B9F7A0B038BD06505712
SHA1:	0D7E42D0733A18A4C48B83EBBC68575925B0CD69

SHA-256:	433F8C545F788D4F901AAD7B70F63700BD6861A1ABE32FAE7C8FD08AE29004BD
SHA-512:	9A3AAEF350767D68BD455F50272BB942A860D3712C831C99896B9814C1733198321B3422D7E411974C56D71DA064716E354BAC0963DFB1D9A786612897A2A4CF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationFramework\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info	
General	
File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.273721496886178
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, flv, cel) (7/3) 0.00%
File name:	file.exe
File size:	2564217
MD5:	b285997d1fb1ed7ff9129e4e9566c2e5
SHA1:	64fe09e86b2e6dc67bb85faf9d7a746976edb4a0
SHA256:	8edce063ac9af61dd0b493b9dec7e959b93021ad55a07cfe6e2b5519b46581f2
SHA512:	d232f632f725ca0351f9c37000f2c3c2f70f2a221e29f33a5e167a9b42d1529ca84f51854a8d9944a4534464f6ec5327b9b01bb46ca5370680f52216d49bef6
SSDEEP:	24576:ZRjcXgYLSaH8MIV0/AGQsHE9IWJnVo2FDq6mZC/36KBsQ96letoreojRqkdvgdBx:Hjh3E7nVoYDv/3DBsQ+dkBx
TLSH:	87C51B036A8B0D75DDD27BB461CB633AA738ED30CA2A9F7FB608C53559532C46C1A742
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..L....87.c.....@Z.....'.....t.....@.....'.....S'....@.....

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info	
General	
Entrypoint:	0x401490
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x63863738 [Tue Nov 29 16:45:44 2022 UTC]
TLS Callbacks:	0x415370, 0x415320
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	26093aeed04a948c138ea9102034d47f

Entrypoint Preview

Instruction
mov dword ptr [00533060h], 00000000h
jmp 00007F93A0BC42C6h
nop
sub esp, 1Ch
mov eax, dword ptr [esp+20h]
mov dword ptr [esp], eax
call 00007F93A0BE7446h
test eax, eax
sete al
add esp, 1Ch
movzx eax, al
neg eax
ret
nop
nop
nop
push ebp
mov ebp, esp
push edi
push esi
push ebx
sub esp, 1Ch
mov dword ptr [esp], 004E6000h
call dword ptr [00534208h]
sub esp, 04h
test eax, eax
je 00007F93A0BC4685h
mov ebx, eax
mov dword ptr [esp], 004E6000h
call dword ptr [00534224h]
mov edi, dword ptr [00534210h]
sub esp, 04h
mov dword ptr [00533020h], eax
mov dword ptr [esp+04h], 004E6013h
mov dword ptr [esp], ebx
call edi
sub esp, 08h
mov esi, eax
mov dword ptr [esp+04h], 004E6029h
mov dword ptr [esp], ebx
call edi
sub esp, 08h
mov dword ptr [004C1004h], eax
test esi, esi
je 00007F93A0BC4623h
mov dword ptr [esp+04h], 00533024h
mov dword ptr [esp], 004F4104h
call esi
mov dword ptr [esp], 00401560h
call 00007F93A0BC4573h
lea esp, dword ptr [ebp-0Ch]
pop ebx
pop esi
pop edi
pop ebp
ret
lea esi, dword ptr [esi+00000000h]
mov eax, 0041AE40h
mov esi, 0000A660h

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x134000	0xa98	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x137000	0x6320	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xed1f4	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1341e4	0x1a8	.idata
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	0xbfd38	0xbfe00	False	0.37507888843648207	data	6.311305933324127	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xc1000	0x247d0	0x24800	False	0.6999678938356164	dBase III DBT, version number 0, next free block index 10, 1st item "D\213k\034B\200\320\321\227\233<\035\214\264\363\270\346\0341\215\342+\356\035_362\2407\313\231""	7.147373481327555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xe6000	0xd7e0	0xd800	False	0.3976236979166667	data	5.768246776593719	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
/4	0xf4000	0x3e014	0x3e200	False	0.20320359657947687	data	4.932991729749517	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x133000	0xbe0	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x134000	0xa98	0xc00	False	0.3707682291666667	data	4.802653247939785	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x135000	0x30	0x200	False	0.060546875	data	0.2233456448570176	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x136000	0x8	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x137000	0x6320	0x6400	False	0.6265625	data	6.629503326426674	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/14	0x13e000	0x110	0x200	False	0.259765625	Matlab v4 mat-file (little endian) *, rows 2, columns 262144	1.4688848769576526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/29	0x13f000	0x114cc	0x11600	False	0.43585600269784175	Matlab v4 mat-file (little endian) \232aA, rows 2, columns 17039360	5.953087124455304	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/41	0x151000	0x1b2d	0x1c00	False	0.2998046875	data	4.934458145598331	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/55	0x153000	0x6bdd	0x6c00	False	0.4019097222222222	data	5.235076571151023	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/67	0x15a000	0x38	0x200	False	0.1171875	data	0.6721446845015864	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/80	0x15b000	0x1ea	0x200	False	0.609375	data	4.817520394014974	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/91	0x15c000	0x7f05	0x8000	False	0.437591552734375	data	5.358754830827274	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/107	0x164000	0x1028	0x1200	False	0.5264756944444444	data	5.155904228339899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports	
DLL	Import
KERNEL32.dll	CloseHandle, CreateSemaphoreW, DeleteCriticalSection, EnterCriticalSection, FormatMessageA, FreeConsole, FreeLibrary, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetModuleHandleW, GetProcAddress, GetStartupInfoA, InitializeCriticalSection, IsDBCSLeadByteEx, LeaveCriticalSection, LoadLibraryA, LoadLibraryW, LocalFree, MultiByteToWideChar, ReleaseSemaphore, SetLastError, SetUnhandledExceptionFilter, Sleep, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, VirtualProtect, VirtualQuery, WaitForSingleObject, WideCharToMultiByte
msvcrt.dll	__getmainargs, __initenv, __mb_cur_max, __p_acmdln, __p_commode, __p_fmode, __set_app_type, __setusermatherr, _amsg_exit, _cexit, _close, _errno, _fdopen, _filelengthi64, _fileno, _fileno, _fstat64, _initterm, _iob, _lseeki64, _onexit, _read, _wopen, _write, abort, atoi, calloc, exit, fclose, fflush, fgetpos, fopen, fprintf, fputc, fputs, fread, free, fsetpos, fwrite, getc, getwc, iswctype, localeconv, malloc, memchr, memcmp, memcpy, memmove, memset, putc, putwc, realloc, setlocale, setvbuf, signal, strchr, strcmp, strcoll, strerror, strtime, strlen, strncmp, strxfrm, tolower, toupper, ungetc, ungetwc, vprintf, wscoll, wcsftime, wcslen, wcsxfrm

Network Behavior								
Snort IDS Alerts								
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP	
192.168.2.3172.86.120.14 64968428192850286 11/30/22-00:11:55.241038	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49684	2819	192.168.2.3	172.86.120.146	
192.168.2.3172.86.120.14 64968428192850027 11/30/22-00:11:30.935107	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49684	2819	192.168.2.3	172.86.120.146	
172.86.120.146192.168.2.32819496842850353 11/30/22-00:11:32.905229	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	2819	49684	172.86.120.146	192.168.2.3	

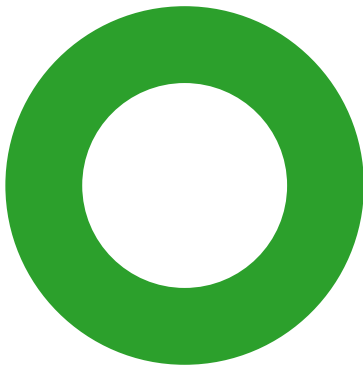
TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:11:30.393584013 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:30.536389112 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:30.536550045 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:30.935106993 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:31.077410936 CET	2819	49684	172.86.120.146	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:11:31.164304972 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:32.762913942 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:32.905229092 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:32.960944891 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:40.604437113 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:40.792125940 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:40.927454948 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:40.927488089 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:40.927510977 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:40.927557945 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:40.976969957 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:42.876482964 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:43.196058989 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:43.337716103 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:43.386504889 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:43.453166008 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:43.594470024 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:43.631895065 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:43.773346901 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:43.821464062 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:43.876497030 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:44.017739058 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:44.034832001 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:44.175971985 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:44.187093019 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:44.329595089 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:44.350819111 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:44.510768890 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:44.555418968 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:45.115401030 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:45.258395910 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:45.310391903 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.084223986 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.225177050 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.225202084 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.225231886 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.225245953 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.225251913 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.225322008 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.225322008 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.276420116 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.276525974 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.366136074 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.366178036 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.366205931 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.366224051 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.366239071 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.366262913 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.366262913 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.366271973 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.366375923 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.366485119 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.366520882 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.417468071 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.417593002 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.507074118 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507108927 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507154942 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507204056 CET	49684	2819	192.168.2.3	172.86.120.146

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:11:49.507246971 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507250071 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.507329941 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.507458925 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507477045 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507505894 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507524014 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507539034 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507556915 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.507584095 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507601023 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507695913 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507716894 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507865906 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507873058 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.507931948 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507949114 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.507953882 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.507992029 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.508111954 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.508132935 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.508236885 CET	49684	2819	192.168.2.3	172.86.120.146
Nov 30, 2022 00:11:49.558928967 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.558964968 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655164003 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655400038 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655414104 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655426025 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655445099 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655457020 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655524969 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655536890 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655729055 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655822039 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655922890 CET	2819	49684	172.86.120.146	192.168.2.3
Nov 30, 2022 00:11:49.655935049 CET	2819	49684	172.86.120.146	192.168.2.3

Statistics

Behavior



- file.exe
- conhost.exe
- vbc.exe



Click to jump to process

System Behavior

Analysis Process: file.exe PID: 5316, Parent PID: 3452

General

Target ID:	0
Start time:	00:11:11
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x3e0000
File size:	2564217 bytes
MD5 hash:	B285997D1FB1ED7FF9129E4E9566C2E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.263012533.00000000010B2000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.263412439.00000000004A2000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

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: 5332, Parent PID: 5316

General

Target ID:	1
Start time:	00:11:11
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: vbc.exe PID: 5384, Parent PID: 5316

General

Target ID:	2
Start time:	00:11:12
Start date:	30/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xa90000
File size:	2688096 bytes

MD5 hash:	B3A917344F5610BEEC562556F11300FA
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: 00000002.00000002.356537948.0000000006AB2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.356537948.0000000006AB2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D17CF06	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	6D17CF06	unknown	
C:\Users\user\AppData\Local\Yandex	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6BFCBEFF	CreateDirectoryW	
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6BFCBEFF	CreateDirectoryW	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\vlc.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D48C78D	CreateFileW	

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\vlc.exe.log	0	2843	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	6D48C907	WriteFile	

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	8173	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	8173	end of file	1	6D15CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore.0f00f0f#889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore.820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase.d5a228c16a218f0d3f02cdcbb8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core.f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.92aa12#34957343ad5d84dae97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml.b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration.8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbcs.exe.config	unknown	8173	end of file	1	6D155705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	6	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	4096	success or wait	12	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	4096	success or wait	24	6BFC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	4096	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	7	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6BFC1B4F	ReadFile
C:\Users\user\Desktop\HQBDRDYKDE.docx	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\Desktop\HQBDRDYKDE.docx	unknown	1022	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\Desktop\SNIPGPPREP.docx	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\Desktop\SNIPGPPREP.docx	unknown	1022	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\Documents\HQBDRDYKDE.docx	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\Documents\HQBDRDYKDE.docx	unknown	1022	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\Documents\SNIPGPPREP.docx	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\Documents\SNIPGPPREP.docx	unknown	1022	end of file	1	6BFC1B4F	ReadFile

Disassembly

 No disassembly