ID: 756115
Sample Name: SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe
Cookbook: default.jbs
Time: 16:49:14
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

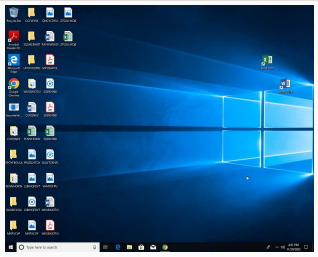
Windows Analysis Report

SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe

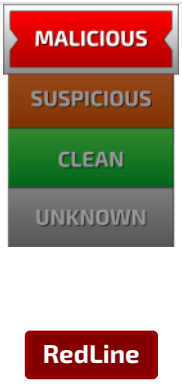
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe
Analysis ID:	756115
MD5:	34a852c0f62294..
SHA1:	6204b0e10eaf80..
SHA256:	f461d11f2fac14f...
Tags:	exe RedLineStealer
Infos:	



Detection



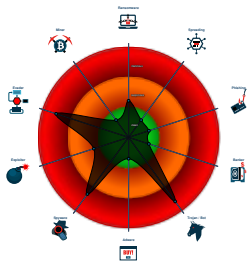
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle...
- Connects to many ports of the same...
- Machine Learning detection for sam...
- Allocates memory in foreign process...
- Injects a PE file into a foreign proce...
- Queries sensitive video device infor...
- Contains functionality to inject code...

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe (PID: 3384 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe MD5: 34A852C0F62294480E1E6E154B00539A)
  - conhost.exe (PID: 3276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vbc.exe (PID: 260 cmdline: C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - conhost.exe (PID: 576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "193.106.191.138:32796"
  ],
  "Authorization Header": "54c79ce081122137049ee07c0a2f38ab"
}
```

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
00000000.00000002.319419057.0000000000415000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000003.318847444.00000000005E2000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.422192402.0000000007777000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe.5e0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe.5e0000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x21068:$pat14: , CommandLine: • 0x18d64:$v2_1: ListOfProcesses • 0x18af8:$v4_3: base64str • 0x19b83:$v4_4: stringKey • 0x16708:$v4_5: BytesToStringConverted • 0x15770:$v4_6: FromBase64 • 0x16edc:$v4_8: procName • 0x1725f:$v5_1: DownloadAndExecuteUpdate • 0x18a08:$v5_2: ITaskProcessor • 0x1724d:$v5_3: CommandLineUpdate • 0x1723e:$v5_4: DownloadUpdate • 0x178f2:$v5_5: FileScanning • 0x16a77:$v5_7: RecordHeaderField • 0x16496:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe.414788.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe.414788.1.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1f468:$pat14: , CommandLine: • 0x17164:$v2_1: ListOfProcesses • 0x16ef8:$v4_3: base64str • 0x17f83:$v4_4: stringKey • 0x14b08:$v4_5: BytesToStringConverted • 0x13b70:$v4_6: FromBase64 • 0x152dc:$v4_8: procName • 0x1565f:$v5_1: DownloadAndExecuteUpdate • 0x16e08:$v5_2: ITaskProcessor • 0x1564d:$v5_3: CommandLineUpdate • 0x1563e:$v5_4: DownloadUpdate • 0x15cf2:$v5_5: FileScanning • 0x14e77:$v5_7: RecordHeaderField • 0x14896:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe.400000.0.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 net.tcp Init - Source IP: 192.168.2.5 - Destination IP: 193.106.191.138

Timestamp:	192.168.2.5193.106.191.13849699327962850027 11/29/22-16:50:39.536972
SID:	2850027
Source Port:	49699
Destination Port:	32796
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 193.106.191.138	
Timestamp:	192.168.2.5193.106.191.1384969932796285028 6 11/29/22-16:51:03.828285
SID:	2850286
Source Port:	49699
Destination Port:	32796
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 193.106.191.138 - Destination IP: 192.168.2.5	
Timestamp:	193.106.191.138192.168.2.532796496992850353 11/29/22-16:50:41.373927
SID:	2850353
Source Port:	32796
Destination Port:	49699
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Connects to many ports of the same IP (likely port scanning)

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

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

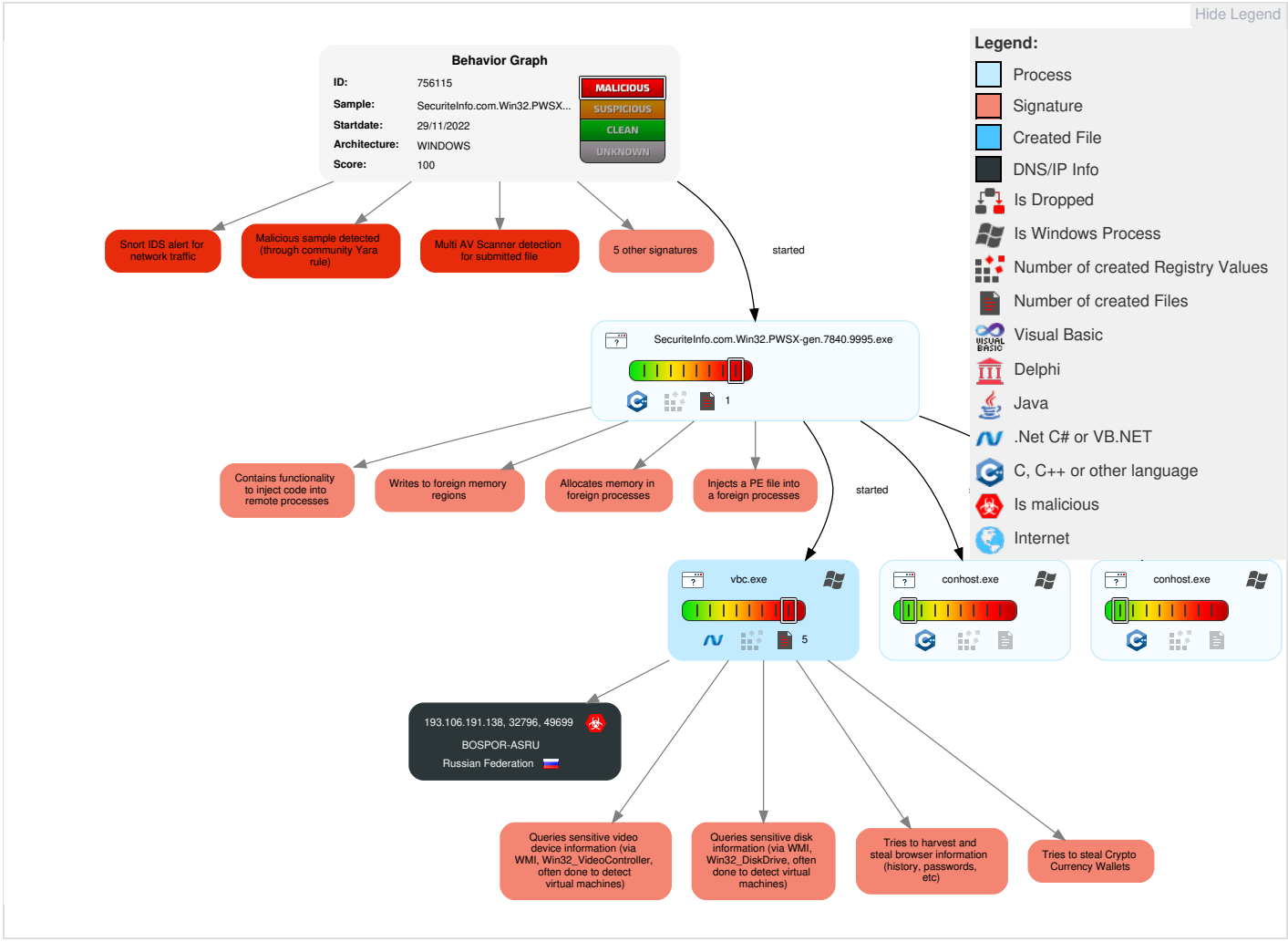
Tries to harvest and steal browser information (history, passwords, etc)

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	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 4 Security Software Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	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	1 1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	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)	4 1 1 Process Injection	NTDS	2 3 1 Virtualization/Sandbox Evasion	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 1 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	Steganography	Cached Domain Credentials	1 3 5 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
SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe	30%	Virustotal		Browse
SecuriteInfo.com.Win32.PWSX-gen.7840.9995.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/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	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	
193.106.191.138:32796	0%	URL Reputation	safe	
193.106.191.138:32796	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/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	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
193.106.191.138:32796	true	• URL Reputation: safe • URL Reputation: safe	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	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	vbc.exe, 00000002.00000002.423894970.0000000007996000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.404603370.0000000008754000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.404090422.0000000008685000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.404056557.000000000880D000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.405554878.000000000883F000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.405444480.0000000008822000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.421928279.0000000007730000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.407871530.00000000087F0000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.403947258.0000000008668000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.406589920.000000000897E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	vbc.exe, 00000002.00000003.406589920.000000000897E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.422192402.0000000007777000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	vbc.exe, 00000002.00000002.422192402.0000000007777000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faulth	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id4	vbc.exe, 00000002.00000002.419721126.00000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	vbc.exe, 00000002.00000002.419721126.00000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	vbc.exe, 00000002.00000002.422192402.0000007777000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	vbc.exe, 00000002.00000002.422192402.0000007777000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	vbc.exe, 00000002.00000002.419721126.00000074E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	vbc.exe, 00000002.00000002.422192402.0000007777000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	vbc.exe, 00000002.00000002.422192402.0000007777000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe, SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe, 00000000.00000002.319419057.00000000415000.00000004.00000001.01000000.00000003.sdmp, vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	vbc.exe, 00000002.00000002.420283444.0000007573000.00000004.00000800.00020000.00000000.sdmp	false		high

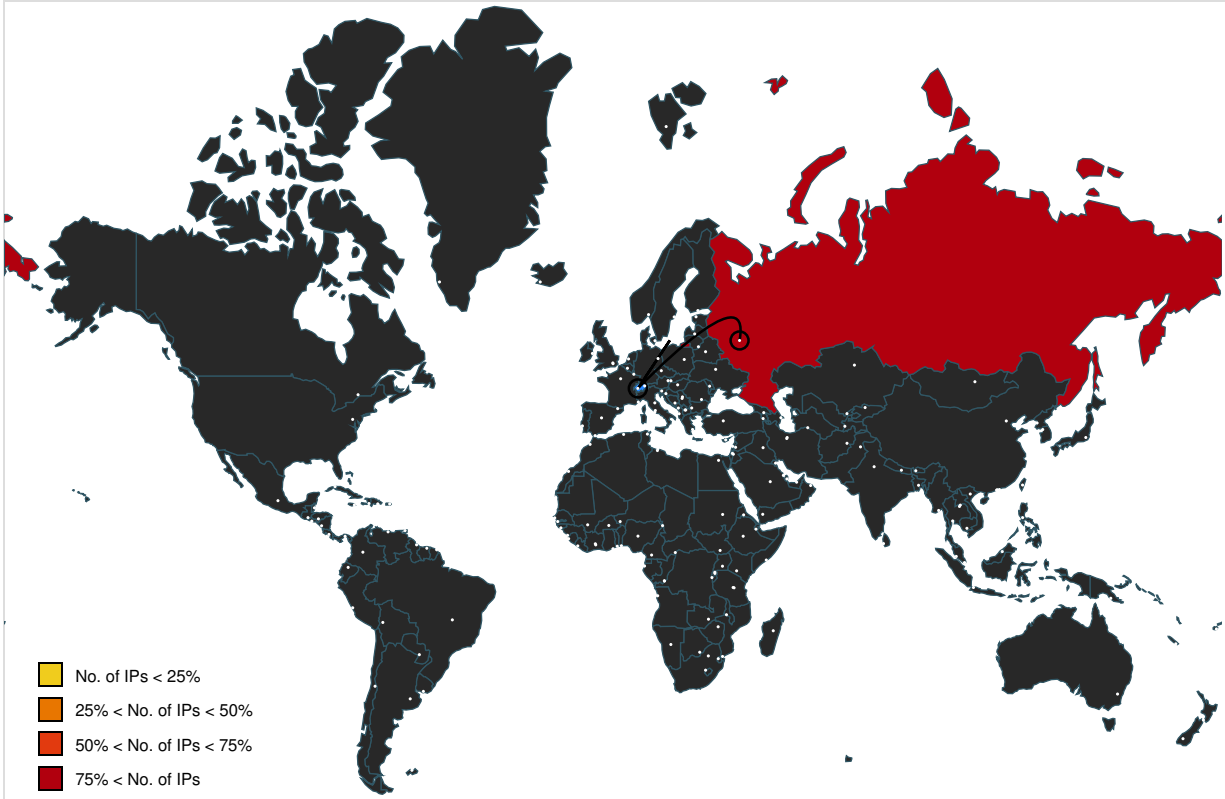
Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id9Response	vbc.exe, 00000002.00000002.422192402.000 0000007777000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.419721126.00000000074E1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// https://duckduckgo.com/favicon.icohttps://duckduckgo. com/?q=	vbc.exe, 00000002.00000003.406589920.000 000000897E000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	vbc.exe, 00000002.00000002.419721126.000 00000074E1000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.419721126.00000000074E1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	vbc.exe, 00000002.00000002.419721126.000 00000074E1000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://tempuri.org/Entity/Id23	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.419721126.00000000074E1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://tempuri.org/Entity/Id24	vbc.exe, 00000002.00000002.419721126.000 00000074E1000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	vbc.exe, 00000002.00000002.419721126.000 00000074E1000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.419721126.00000000074E1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	vbc.exe, 00000002.00000002.423894970.000 0000007996000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 03.404603370.0000000008754000.00000004.0 0000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.404090422.00000000086 85000.00000004.00000800.00020000.0000000 0.sdmp, vbc.exe, 00000002.00000003.40805 6557.000000000880D000.00000004.00000800. 00020000.00000000.sdmp, vbc.exe, 0000000 2.00000003.405554878.000000000883F000.00 000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.405444480.000 0000008822000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.421928279.0000000007730000.00000004.0 0000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.407871530.00000000087 F0000.00000004.00000800.00020000.0000000 0.sdmp, vbc.exe, 00000002.00000003.40394 7258.0000000008668000.00000004.00000800. 00020000.00000000.sdmp, vbc.exe, 0000000 2.00000003.406589920.000000000897E000.00 000004.00000800.00020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	vbc.exe, 00000002.00000002.419721126.000 00000074E1000.00000004.00000800.00020000 .00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	vbc.exe, 00000002.00000002.422192402.0000000007777000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	vbc.exe, 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	vbc.exe, 00000002.00000002.419721126.00000000074E1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id10Response	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.422192402.0000000007777000.00000004.0 0000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000002.419721126.00000000074 E1000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	vbc.exe, 00000002.00000002.422192402.000 0000007777000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.419721126.00000000074E1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	vbc.exe, 00000002.00000002.419721126.000 00000074E1000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	vbc.exe, 00000002.00000002.423894970.000 0000007996000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 03.404603370.0000000008754000.00000004.0 0000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.404090422.00000000086 85000.00000004.00000800.00020000.0000000 0.sdmp, vbc.exe, 00000002.00000003.40805 6557.000000000880D000.00000004.00000800. 00020000.00000000.sdmp, vbc.exe, 0000000 2.00000003.405554878.000000000883F000.00 000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.405444480.000 0000008822000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.421928279.0000000007730000.00000004.0 0000800.00020000.00000000.sdmp, vbc.exe, 00000002.00000003.407871530.00000000087 F0000.00000004.00000800.00020000.0000000 0.sdmp, vbc.exe, 00000002.00000003.40394 7258.0000000008668000.00000004.00000800. 00020000.00000000.sdmp, vbc.exe, 0000000 2.00000003.406589920.000000000897E000.00 000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://tempuri.org/Entity/Id23Response	vbc.exe, 00000002.00000002.422192402.000 0000007777000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000002.000000 02.419721126.00000000074E1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/06/addressingex	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	vbc.exe, 00000002.00000002.420283444.000 0000007573000.00000004.00000800.00020000 .00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756115
Start date and time:	2022-11-29 16:49:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.PWSX-gen.7840.9995.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:	5
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@5/1@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 90.9% (good quality ratio 87.2%) • Quality average: 82.3% • Quality standard deviation: 25.7%
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 • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target vbc.exe, PID 260 because it is empty
- 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
16:50:51	API Interceptor	23x 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:MxHKXeHKIEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHKx1qHjW:iqXeqm00YqhQnouOqLqdqNq2qzcGtlxM
MD5:	E787CF7FE6F73C60B1ADCB6CFE9A2FAE
SHA1:	CF44D405D677875BC3AC3A41336DA6C8F3E58277
SHA-256:	6332B18367739773EAA1686C22A11DCEAD2D7314EBCEE5510F5E6A799A301203
SHA-512:	8C7213E33F6A56744FAED770ECC85BFC0F9DF1EA07249CFA6FDFD1EB0822F0ADD47BB072EE21CA6442D03A1E44FE2613BFC4FFC4B72B029F33AA292A390F02 3B
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\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf 3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"Present ationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f #\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\f1d8480152e0da9a60ad49c6d16a3b6d\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):	7.344808175573031
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe
File size:	221696
MD5:	34a852c0f62294480e1e6e154b00539a
SHA1:	6204b0e10eaf8094da16cb5ca7c325f1dbfa97f0
SHA256:	f461d11f2fac14f49aeedd66999b404cfce4138d27fe7e1da79f0aa85eee5149
SHA512:	3d1edf618361a6544937b7c2e5f74bc0d7793d5eb1738ccc3a5d47cf1819efd6ca4bd4bd55d883b7826ee59c6dd6287b5a611d4d4dcdd7a788e260a2c821bea4
SSDEEP:	3072:ehbc8yCxsFNcEyyrJ9WU4khLTvPZFzD0yfZNuzK/hRp1d53CDX5dINLqVqU:VCxGNp7FUyf2AhZjwINut
TLSH:	F124CF1AF5621232DE6AE0F855C1CBD4603D66B2AF81400A7F2D0F7F6D3A0D7729635A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....v...v...v...$...v...$...v.....v...$...v.....v..ty...v...v...v.....v...$...v.....v..Rich.v.....PE..L...X..c...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x406252
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x63860258 [Tue Nov 29 13:00:08 2022 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:	bcac65c952b8ab1f885fe93835602555

Entrypoint Preview

Instruction
call 00007FF934D37E1Ah
jmp 00007FF934D35A49h
mov edi, edi
push esi
push 00000001h
push 00436BA0h
mov esi, ecx
call 00007FF934D37E9Ah
mov dword ptr [esi], 00410B84h
mov eax, esi
pop esi
ret
mov dword ptr [ecx], 00410B84h
jmp 00007FF934D37EFFh
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
mov dword ptr [esi], 00410B84h
call 00007FF934D37EECh
test byte ptr [ebp+08h], 00000001h
je 00007FF934D35BA9h
push esi
call 00007FF934D37F55h
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FF934D37E6Bh
mov dword ptr [esi], 00410B84h
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0Ch
jmp 00007FF934D35BAFh
push dword ptr [ebp+08h]
call 00007FF934D3818Fh

Instruction
pop ecx
test eax, eax
je 00007FF934D35BB1h
push dword ptr [ebp+08h]
call 00007FF934D380A9h
pop ecx
test eax, eax
je 00007FF934D35B88h
leave
ret
test byte ptr [00437C08h], 00000001h
mov esi, 00437BFCh
jne 00007FF934D35BBBh
or dword ptr [00437C08h], 01h
mov ecx, esi
call 00007FF934D35AF9h
push 0040F8B3h
call 00007FF934D38016h
pop ecx
push esi
lea ecx, dword ptr [ebp-0Ch]
call 00007FF934D45B32h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2008 SP1 build 30729 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 SP1 build 30729 • [RES] VS2008 build 21022 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x128a4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x39000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x10000	0x150	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xe8c7	0xea00	False	0.5349726228632479	data	6.652448585777237	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x10000	0x3092	0x3200	False	0.48296875	data	6.068435754636973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x14000	0x247d8	0x23c00	False	0.7369017701048951	Alpha compressed COFF	7.268563044922397	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x39000	0x600	0x600	False	0.455078125	data	3.9776323787735532	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x39200	0x3fc	data	English	United States
RT_MANIFEST	0x390a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetLogicalDrives, CreateEventW, GetProcessHeap, QueryPerformanceFrequency, AreFileApisANSI, GetVersion, CreateFileW, GetCurrentProcess, CreateMutexW, IsProcessorFeaturePresent, FreeConsole, MultiByteToWideChar, GetModuleHandleA, GetProcAddress, GetCommandLineA, SetUnhandledExceptionFilter, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetLastError, GetEnvironmentStringsW, SetHandleCount, GetFileType, GetStartupInfoA, DeleteCriticalSection, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, HeapFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapAlloc, RaiseException, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, TerminateProcess, UnhandledExceptionFilter, IsDebuggerPresent, LeaveCriticalSection, EnterCriticalSection, LoadLibraryA, InitializeCriticalSectionAndSpinCount, VirtualAlloc, HeapReAlloc, RtlUnwind, HeapSize, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA
WINSPOOL.DRV	FindFirstPrinterChangeNotification, FindClosePrinterChangeNotification, FindNextPrinterChangeNotification, WritePrinter, ScheduleJob
COMCTL32.dll	ImageList_Remove, ImageList_ReplaceIcon, InitCommonControlsEx, ImageList_Destroy, ImageList_Create, ImageList_SetBkColor, CreateToolbarEx

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5193.106.191.138496993279628500271/29/22-16:50:39.536972	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49699	32796	192.168.2.5	193.106.191.138
192.168.2.5193.106.191.138496993279628502861/29/22-16:51:03.828285	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49699	32796	192.168.2.5	193.106.191.138
193.106.191.138192.168.2.532796496992850353 11/29/22-16:50:41.373927	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	32796	49699	193.106.191.138	192.168.2.5

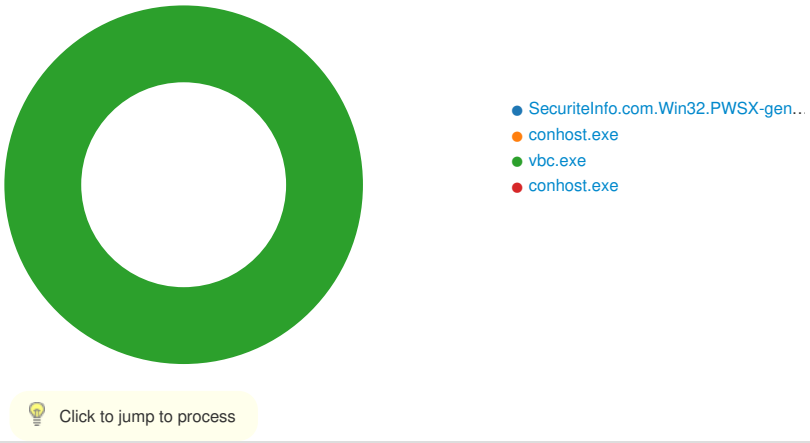
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:39.047336102 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:39.105020046 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:50:39.105655909 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:39.536972046 CET	49699	32796	192.168.2.5	193.106.191.138

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:39.595108986 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:50:39.677771091 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:41.315479040 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:41.373927116 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:50:41.427968979 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:48.698524952 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:48.765489101 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:50:48.765543938 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:50:48.765574932 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:50:48.766961098 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:50.490920067 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:50:50.550380945 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:50:50.601082087 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:01.042223930 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:01.100651026 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:01.179604053 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:01.918889046 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:01.990061998 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.015486002 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.073432922 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.268264055 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.328644037 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.328670979 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.328689098 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.447978973 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.505686045 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.511476040 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.569384098 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.572211981 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.630630016 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.680166006 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.772866011 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.831033945 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.853375912 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:02.911556005 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:02.976716995 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.070801973 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.128408909 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.129113913 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.159497976 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.217700005 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.306329966 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.364243984 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.476902008 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.565983057 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.625777960 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.649928093 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.707921982 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.710012913 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.767947912 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.769047976 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.826925039 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.828284979 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:03.886820078 CET	32796	49699	193.106.191.138	192.168.2.5
Nov 29, 2022 16:51:03.976751089 CET	49699	32796	192.168.2.5	193.106.191.138
Nov 29, 2022 16:51:04.092643023 CET	49699	32796	192.168.2.5	193.106.191.138

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe PID: 3384, Parent PID: 3324

General

Target ID:	0
Start time:	16:50:17
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.7840.9995.exe
Imagebase:	0x400000
File size:	221696 bytes
MD5 hash:	34A852C0F62294480E1E6E154B00539A
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: 00000000.00000002.319419057.0000000000415000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.318847444.00000000005E2000.00000040.00001000.00020000.00000000.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: 3276, Parent PID: 3384

General

Target ID:	1
Start time:	16:50:17
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7fcd70000
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: **260**, Parent PID: **3384**

General

Target ID:	2
Start time:	16:50:18
Start date:	29/11/2022
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:	0x1320000
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: 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.420283444.0000000007573000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.422192402.0000000007777000.00000004.00000800.00020000.00000000.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	6C98CF06	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	6C98CF06	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	6B7DBEFF	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	6B7DBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC9C78D	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\vbc.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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	6CC9C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C965705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C8C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6C96CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6C96CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C96CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C8C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6C965705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C8C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B7D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	success or wait	1	6B7D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6B7D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	163	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	11	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	6	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6B7D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6B7D1B4F	ReadFile

Analysis Process: conhost.exe PID: **576**, Parent PID: **3384**

General

Target ID:	4
Start time:	16:51:05
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly