ID: 323824
Sample Name:
SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.28577
Cookbook: default.jbs
Time: 15:50:11
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

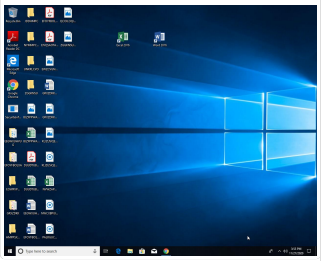
Analysis Report SecuriteInfo.com.Trojan.PWS.Stealer.29…

Overview

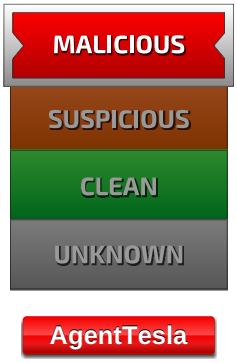
General Information

Sample Name:	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.28577 (renamed file extension from 28577 to exe)
Analysis ID:	323824
MD5:	224e779ff4d39ce..
SHA1:	e248c7182cbfb66..
SHA256:	92d9b1922bebbb..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

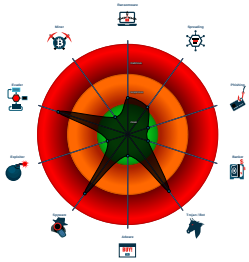


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- May check the online IP address of …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe (PID: 3148 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe' MD5: 224E779FF4D39CE90878AE3E630197E7)
  - SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe (PID: 2844 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe MD5: 224E779FF4D39CE90878AE3E630197E7)
- vlc.exe (PID: 4120 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 224E779FF4D39CE90878AE3E630197E7)
  - vlc.exe (PID: 6384 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 224E779FF4D39CE90878AE3E630197E7)
  - vlc.exe (PID: 6400 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 224E779FF4D39CE90878AE3E630197E7)
- vlc.exe (PID: 6268 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 224E779FF4D39CE90878AE3E630197E7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "D1veT2GUQ",
  "URL: ": "https://6Myp18QaIbJyfOWJxc.com",
  "To: ": "",
  "ByHost: ": "mail.baharanvilla.ir:587",
  "Password: ": "SrT57YCz2",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.505770238.0000000002B01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.505770238.0000000002B01000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.263990752.000000000312 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.500003272.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.505873536.0000000002B5 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

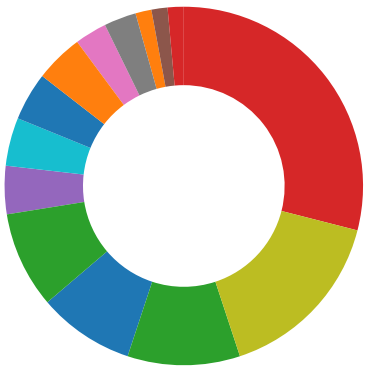
Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.vlc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Spreading
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

May check the online IP address of the machine

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

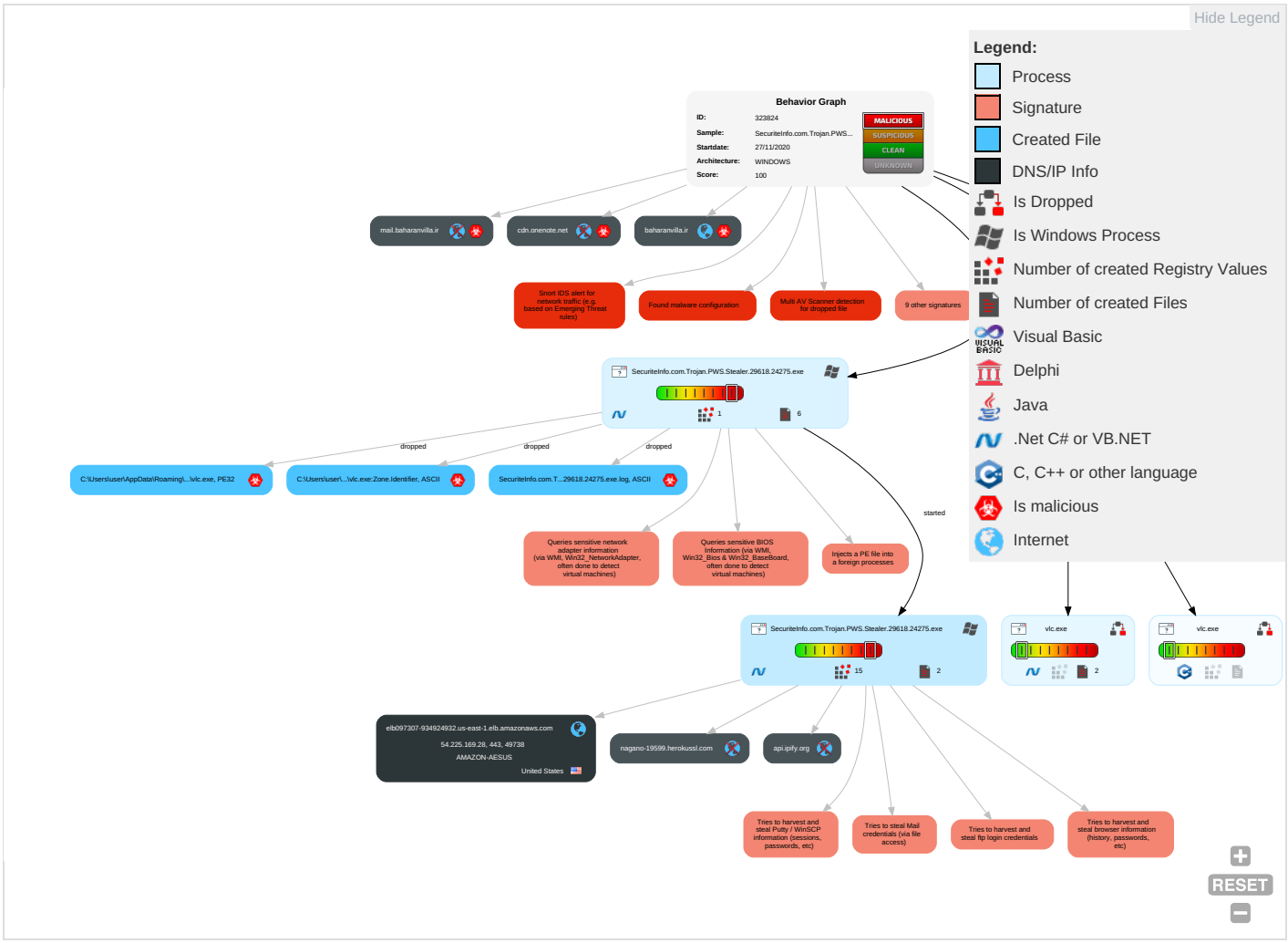
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 2 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 2 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

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.Trojan.PWS.Stealer.29618.24275.exe	31%	Virustotal		Browse
SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe	38%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	
SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	38%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
baharanvilla.ir	2%	Virustotal		Browse
cdn.onenote.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://mail.baharanvilla.ir	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/yq	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.typography.net-u	0%	Avira URL Cloud	safe	
http://www.typography.netw~	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comnap/	0%	Avira URL Cloud	safe	
http://www.urwpp.deFT	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/R	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0t0	0%	Avira URL Cloud	safe	
http://www.typography.netlique	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/1q	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sakkal.com0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.fontbureau.comcomF	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/Tq9sp	0%	Avira URL Cloud	safe	
http://www.typography.nett	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/:qWs	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krrsy	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Cq	0%	Avira URL Cloud	safe	
http://www.typography.netief	0%	Avira URL Cloud	safe	
http://https://6Myp18QaIbJyfOWJxc.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueedoq$s$	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comTCQ	0%	Avira URL Cloud	safe	
http://www.carterandcone.com1	0%	Avira URL Cloud	safe	
http://IMzSbX.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-ca(qes	0%	Avira URL Cloud	safe	
http://www.fontbureau.commyq	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.typography.netK~	0%	Avira URL Cloud	safe	
http://www.fontbureau.comT.TTF	0%	Avira URL Cloud	safe	
http://www.carterandcone.comrl	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://schemas.microso	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmI	0%	Avira URL Cloud	safe	
http://www.fonts.comp	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/O	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.225.169.28	true	false		high
baharanvilla.ir	185.165.40.194	true	true	• 2%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high
mail.baharanvilla.ir	unknown	unknown	true		unknown
cdn.onenote.net	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.505770238.000000002B01000.00000004.00000001.sdmp, vlc.exe, 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersL6	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.244267564.000000005E2E000.00000004.00000001.sdmp	false		high
http://mail.baharanvilla.ir	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.507519954.000000002DBC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd9	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239403264.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/yq	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.235672179.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238679080.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false		high
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersers	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238939245.000000005E2E000.00000004.00000001.sdmp	false		high
http://www.typography.net-u	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232850879.000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238595635.000000005E14000.00000004.00000001.sdmp	false		high
http://www.typography.netw~	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232850879.000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comnap/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238565181.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deFT	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240089803.000000005DF2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.505770238.0000000002B01000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.263990752.000000003129000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.500003272.0000000000402000.00000040.00000001.sdmp, vlc.exe, 00000005.00000002.314707894.00000000026E8000.00000004.00000001.sdmp, vlc.exe, 0000000D.00000002.500027054.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240839268.000000005E12000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240891546.0000000005E12000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240847379.0000000005DFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.505770238.0000000002B01000.00000004.00000001.sdmp, vlc.exe, 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/R	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.236395168.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0t0	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.235672179.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netlique	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232879628.000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/1q	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.237159352.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com0	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.237106452.000000005E36000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers96-s	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239940201.000000005E2E000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/t	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.237159352.000000005E14000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comcomF	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239333550.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/Tq9sp	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240839268.000000005E12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.nett	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232879628.000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/:qWs	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.237159352.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krrsy	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.233475482.000000005DFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000059E0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Cq	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.236224002.0000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netief	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232879628.0000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://6Myp18QaIbJyfOWJxc.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.505873536.0000000002B55000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.507621145.0000000002DC9000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comueedoq$s$	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238874107.0000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comTCQ	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.234655964.0000000005DF2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com1	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.234598135.0000000005DF2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://IMzSbX.com	vlc.exe, 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/-ca(qes	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.237159352.0000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.commyq	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239059251.0000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.234655964.0000000005DF2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netK~	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232850879.0000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersU	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238855975.0000000005E2E000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comT.TTF	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240319258.0000000005E13000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comrl	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.234598135.0000000005DF2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.orgGETMozilla/5.0	vlc.exe, 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.microso	vlc.exe	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers#6Gs	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239721532.0000000005E2E000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.241174877.0000000005DF2000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.505770238.0000000002B01000.00000004.00000001.sdmp	false		high
http://fontfabrik.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comB.TTF	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239451545.0000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmI	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.260481176.0000000005DF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comp	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232604882.0000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240089803.0000000005DF2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.505770238.0000000002B01000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000059E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238626941.0000000005E14000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/O	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240847379.0000000005DFB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	vlc.exe, 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239207194.0000000005E14000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/fq	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.236224002.0000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/tTq9sp	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.237950566.0000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comCq	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.240319258.0000000005E13000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comce9	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.244250202.0000000005E12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerss7	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238577684.0000000005E2E000.00000004.00000001.sdmp	false		high
http://baharanvilla.ir	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.507519954.0000000002DBC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netrz	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.233119604.0000000005E0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.236224002.0000000005E14000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.coma	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.244296179.000000005E12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wikip	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.232384565.000000005E13000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239451545.000000005E14000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238986582.0000000005E14000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000059E0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.263990752.000000003129000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.500003272.0000000000402000.00000040.00000001.sdmp, vlc.exe, 00000005.00000002.314707894.00000000026E8000.00000004.00000001.sdmp, vlc.exe, 0000000D.00000002.500027054.0000000000402000.00000040.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.237159352.000000005E14000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000059E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comiono	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239059251.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239451545.000000005E14000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000002.270119765.000000007102000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239224806.0000000005E2E000.00000004.00000001.sdmp, vlc.exe, 00000005.00000002.320148424.0000000005680000.00000002.00000001.sdmp, vlc.exe, 0000000A.00000002.323690888.00000000059E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comd?	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239263737.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.505816927.000000002B3B000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.238553956.000000005E2E000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000002.00000002.505770238.000000002B01000.00000004.00000001.sdmp, vlc.exe, 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comsief	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.239550906.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/yq	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe, 00000000.00000003.236224002.000000005E14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.225.169.28	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323824
Start date:	27.11.2020
Start time:	15:50:11
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 12m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.28577 (renamed file extension from 28577 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
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@9/4@5/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.64.90.137, 95.101.184.67, 51.11.168.160, 2.20.142.210, 2.20.142.209, 20.54.26.129, 92.122.213.247, 92.122.213.194, 184.24.28.12, 184.24.7.187 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, cdn.onenote.net.edgekey.net, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:51:26	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
15:51:35	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
15:51:44	API Interceptor	653x Sleep call for process: SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe modified
15:52:08	API Interceptor	492x Sleep call for process: vlc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.225.169.28	5C.exe	Get hash	malicious	Browse	• api.ipify.org/
	Bc.exe	Get hash	malicious	Browse	• api.ipify.org/
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• api.ipify.org/
	Machine drawing.exe	Get hash	malicious	Browse	• api.ipify.org/
	26VT73zxnr.exe	Get hash	malicious	Browse	• api.ipify.org/
	SecuriteInfo.com.Trojan.Inject4.5025.20792.exe	Get hash	malicious	Browse	• api.ipify.org/
	Jeveeagp4.exe	Get hash	malicious	Browse	• api.ipify.org/
	gunzipped.exe	Get hash	malicious	Browse	• api.ipify.org/
	zU4HDC7vYA.exe	Get hash	malicious	Browse	• api.ipify.org/
	InquirySW23020KT.com.exe	Get hash	malicious	Browse	• api.ipify.org/
	Commercial Invoice73802,PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	Purchase Order.exe	Get hash	malicious	Browse	• api.ipify.org/
	PO-0561.exe	Get hash	malicious	Browse	• api.ipify.org/
	SecuriteInfo.com.Trojan.PackedNET.424.9536.exe	Get hash	malicious	Browse	• api.ipify.org/
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	• api.ipify.org/
	update.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	Purchase Order.scr.exe	Get hash	malicious	Browse	• api.ipify.org/
	PO #154469-70.exe	Get hash	malicious	Browse	• api.ipify.org/
	QN27UyUjZ5.exe	Get hash	malicious	Browse	• api.ipify.org/
	RFQ & SAMPLES PRODUCTS 9-1009-GRGS 403.2MT STR20.pdf.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	SecuriteInfo.com.Trojan.MulDrop15.61981.23282.exe	Get hash	malicious	Browse	• 54.235.142.93
	ORDER.exe	Get hash	malicious	Browse	• 54.243.164.148
	swift copy.exe	Get hash	malicious	Browse	• 23.21.42.25
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	lxpo.exe	Get hash	malicious	Browse	• 54.204.14.42
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	SecuriteInfo.com.Variant.Bulz.233365.3916.exe	Get hash	malicious	Browse	• 23.21.252.4
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 54.225.169.28
	INVOICE.xlsx	Get hash	malicious	Browse	• 54.204.14.42
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	1125_56873981.doc	Get hash	malicious	Browse	• 54.243.161.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
baharanvilla.ir	SecuriteInfo.com.Variant.Bulz.233365.3916.exe	Get hash	malicious	Browse	• 185.165.40.194
	BQoFEXaNOEtJ9dC.exe	Get hash	malicious	Browse	• 185.165.40.194

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	SecuriteInfo.com.Trojan.MulDrop15.61981.23282.exe	Get hash	malicious	Browse	• 54.235.142.93
	ORDER.exe	Get hash	malicious	Browse	• 54.243.164.148
	swift copy.exe	Get hash	malicious	Browse	• 23.21.42.25
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 34.231.129.212
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 52.205.236.122
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 35.174.78.146
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 3.215.226.95
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 54.83.52.76
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	http://https://webnavigator.co/?adprovider=AppFocus1&source=d-cp11560482685&group=cg60&device=c&keyword=&creative=477646941053&adposition=none&placement=www.123homeschool4me.com&target=segment_be_a_7802457135858218830&sl=&caid=11560482685&gw=1&test=%3a%2f%2fmail	Get hash	malicious	Browse	• 54.90.26.145
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0Nlk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0lnkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8l8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLlvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUlj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXlfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 34.236.142.3
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJIEgydRUHiWwDj8GYDCxqGnV0O0rI4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMIL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 52.202.11.207

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	Purchase Order.exe	Get hash	malicious	Browse	• 54.225.169.28
	SecuriteInfo.com.Trojan.MulDrop15.61981.23282.exe	Get hash	malicious	Browse	• 54.225.169.28
	ORDER.exe	Get hash	malicious	Browse	• 54.225.169.28
	Mixtec New Order And Price List Requsting Form_pdf.exe	Get hash	malicious	Browse	• 54.225.169.28
	swift copy.exe	Get hash	malicious	Browse	• 54.225.169.28
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.225.169.28
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 54.225.169.28
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 54.225.169.28
	guy1.exe	Get hash	malicious	Browse	• 54.225.169.28
	guy2.exe	Get hash	malicious	Browse	• 54.225.169.28
	Exodus.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.169.28
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.225.169.28
	Order 51897.exe	Get hash	malicious	Browse	• 54.225.169.28
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 54.225.169.28
	98650107.pdf.exe	Get hash	malicious	Browse	• 54.225.169.28
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 54.225.169.28
	Izezma64.dll	Get hash	malicious	Browse	• 54.225.169.28
	fuxenm32.dll	Get hash	malicious	Browse	• 54.225.169.28
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 54.225.169.28

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1391
Entropy (8bit):	5.344111348947579
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4W:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzh
MD5:	E87C60A24438CC611338EA5ACB433A0A
SHA1:	E0C6A7D5CFE32BB2178E71DEE79971A51697B7DD
SHA-256:	80DAB47D7A9E233A692D10ACAF5793E34911836D36DB2E11BB7C5D42DE39782A
SHA-512:	3DBD6773153DC9D05558ED491A92C9B4B72D594263D7BD2D06BDDCF09BE55477D35041145219A5E9A46B38575E5B60DA91C6870B2CA29A83388695AD389B8EE
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	5.344111348947579
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4W:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzh
MD5:	E87C60A24438CC611338EA5ACB433A0A
SHA1:	E0C6A7D5CFE32BB2178E71DEE79971A51697B7DD
SHA-256:	80DAB47D7A9E233A692D10ACAF5793E34911836D36DB2E11BB7C5D42DE39782A
SHA-512:	3DBD6773153DC9D05558ED491A92C9B4B72D594263D7BD2D06BDDCF09BE55477D35041145219A5E9A46B38575E5B60DA91C6870B2CA29A83388695AD389B8EE
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	248832
Entropy (8bit):	7.944818129285475
Encrypted:	false
SSDEEP:	6144:tUEq9SvnCllBvQ1Q2Yc08zqgRqYKZqj7buFP24oeu8:u2n/B4+XyRqRgOBoez
MD5:	224E779FF4D39CE90878AE3E630197E7
SHA1:	E248C7182CBFB6679AB327BBE77A9EB469121AC8
SHA-256:	92D9B1922BEBBB60F7CA75EB99220F92BBDF687AF32A4A966EC90FD562DFE96E
SHA-512:	BC99E47A6BD073C19DEDB989B4CB9557367C40C120BEB1769FDE5C9FF828B61FB32132E53727F0CA7852236222937F5A5048267E2886AE1AF1D6BE7083D843C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...b)._..... ....@.. ....@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....1...5.....b...f...o.....0..y.....(....8....8.....E....8...I...I...83....(.... ....:....& ....8.....(.... .....9....&8.....(.... ....8....*.(....8.....0..-..... .....8.....E.....".....8...*s..... ....(....9....&8.....o....8\.....(....r...p.....(.....(.....o.....o....t....}.... ....8U...8W... ....(....9A...& ....86... ....8%....(.... ....(....9....&8

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.944818129285475
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe
File size:	248832
MD5:	224e779ff4d39ce90878ae3e630197e7

General

SHA1:	e248c7182cbfb6679ab327bbe77a9eb469121ac8
SHA256:	92d9b1922bebbb60f7ca75eb99220f92bbdf687af32a4a966ec90fd562dfe96e
SHA512:	bc99e47a6bd073c19dedb989b4cb9557367c40c120beb1769fde5c9ff828b61fb32132e53727f0ca7852236222937f5a5048267e2886ae1af1d6be7083d843c5
SSDEEP:	6144:tUEq9SvnCIlBvQ1Q2Yc08zqgRqYKZqj7buFP24oeu8:u2n/B4+XyRqRgOBoez
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...b)._................................. ....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x43d60e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC02962 [Thu Nov 26 22:17:06 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3d5c0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0xf80	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x40000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x3b614	0x3b800	False	0.970099954044	data	7.96339396764	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x3e000	0xf80	0x1000	False	0.387939453125	data	5.01100872549	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x40000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3e0a0	0x288	data		
RT_MANIFEST	0x3e328	0xc55	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	Nmsdmwkbi4.exe
FileVersion	1.0.0.0
ProductName	VideoLAN
ProductVersion	1.0.0.0

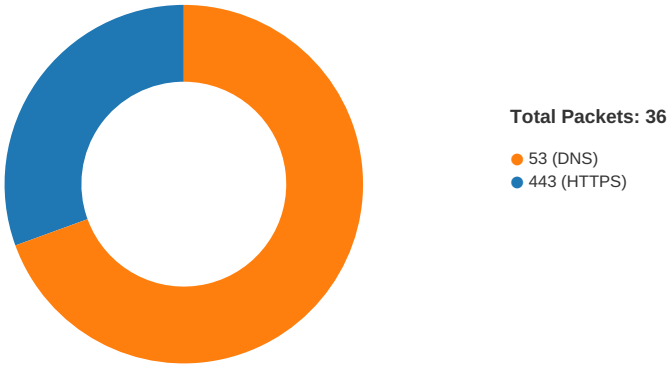
Description	Data
FileDescription	
OriginalFilename	Nmsdmwkbi4.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/27/20-15:53:18.649493	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49739	587	192.168.2.3	185.165.40.194

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:53:06.855217934 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:06.958154917 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:06.958297968 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:07.040256977 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:07.143094063 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.143204927 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.143223047 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.143238068 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.143254042 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.143377066 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:07.144329071 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.194504023 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:07.297736883 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.340001106 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:07.592104912 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:07.700268030 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:07.761272907 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:16.866636992 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:16.969662905 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:16.969686031 CET	443	49738	54.225.169.28	192.168.2.3
Nov 27, 2020 15:53:16.969767094 CET	49738	443	192.168.2.3	54.225.169.28
Nov 27, 2020 15:53:16.969805002 CET	49738	443	192.168.2.3	54.225.169.28

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:51:05.509145975 CET	63492	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:05.536328077 CET	53	63492	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:51:06.215003014 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:06.242132902 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:14.740252018 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:14.767283916 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:15.785001040 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:15.811896086 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:16.461648941 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:16.496841908 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:17.609884977 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:17.637248993 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:18.685058117 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:18.713570118 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:19.470622063 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:19.506201029 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:20.140036106 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:20.167078018 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:21.098515034 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:21.125668049 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:23.169857979 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:23.205410004 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:30.008042097 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:30.044953108 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:32.894954920 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:32.921994925 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:53.416748047 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:53.453550100 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 15:51:59.918345928 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:51:59.961668015 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 15:52:08.657661915 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:52:08.684873104 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 15:52:14.514172077 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:52:14.551282883 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 15:52:46.668731928 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:52:46.695820093 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 15:52:48.720047951 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:52:48.757924080 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 15:53:06.645328045 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:53:06.672275066 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 15:53:06.695077896 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:53:06.730554104 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 15:53:16.879842043 CET	60633	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:53:16.915517092 CET	53	60633	8.8.8.8	192.168.2.3
Nov 27, 2020 15:53:16.969113111 CET	61292	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:53:17.004719019 CET	53	61292	8.8.8.8	192.168.2.3
Nov 27, 2020 15:53:19.707268953 CET	63619	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:53:19.707710981 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 15:53:19.744808912 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 15:53:19.746594906 CET	53	63619	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:53:06.645328045 CET	192.168.2.3	8.8.8.8	0x5cc5	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.695077896 CET	192.168.2.3	8.8.8.8	0xca06	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:16.879842043 CET	192.168.2.3	8.8.8.8	0x250c	Standard query (0)	mail.bahar anvilla.ir	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:16.969113111 CET	192.168.2.3	8.8.8.8	0xe898	Standard query (0)	mail.bahar anvilla.ir	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:19.707710981 CET	192.168.2.3	8.8.8.8	0x94c	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.672275066 CET	8.8.8.8	192.168.2.3	0x5cc5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:06.730554104 CET	8.8.8.8	192.168.2.3	0xca06	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:16.915517092 CET	8.8.8.8	192.168.2.3	0x250c	No error (0)	mail.baharanvilla.ir	baharanvilla.ir		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:53:16.915517092 CET	8.8.8.8	192.168.2.3	0x250c	No error (0)	baharanvilla.ir		185.165.40.194	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:17.004719019 CET	8.8.8.8	192.168.2.3	0xe898	No error (0)	mail.baharanvilla.ir	baharanvilla.ir		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:53:17.004719019 CET	8.8.8.8	192.168.2.3	0xe898	No error (0)	baharanvilla.ir		185.165.40.194	A (IP address)	IN (0x0001)
Nov 27, 2020 15:53:19.744808912 CET	8.8.8.8	192.168.2.3	0x94c	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

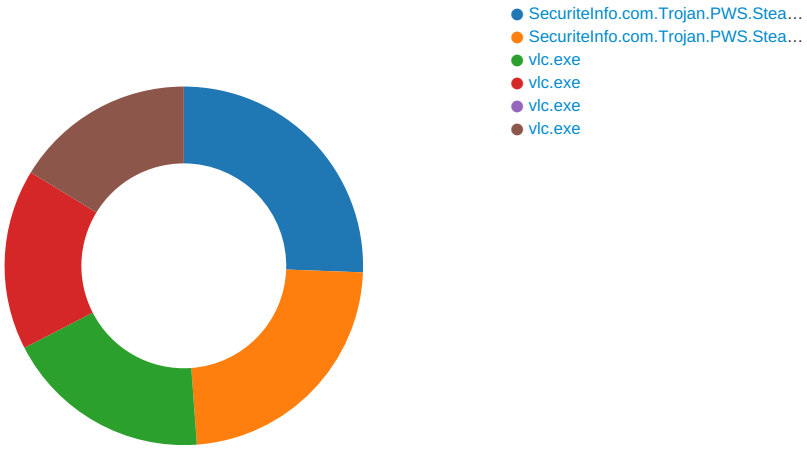
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 15:53:07.144329071 CET	54.225.169.28	443	192.168.2.3	49738	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe PID: 3148
Parent PID: 5536

General

Start time:	15:51:11
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe'
Imagebase:	0xa50000
File size:	248832 bytes
MD5 hash:	224E779FF4D39CE90878AE3E630197E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.263990752.0000000003129000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.264115098.00000000040A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD0BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	79D498B	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	79D498B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 62 29 c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 0b 00 00 b8 03 00 00 12 00 00 00 00 00 00 0e d6 03 00 00 20 00 00 00 e0 03 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 04 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...b)._.......... ....@.. ....@................	success or wait	2	79D498B	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	79D498B	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe.log	unknown	1391	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	vlc	unicode	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"	success or wait	1	6CD0646A	RegSetValueExW

Analysis Process: SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe PID: 2844
Parent PID: 3148

General

Start time:	15:51:25
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe
Imagebase:	0x790000
File size:	248832 bytes
MD5 hash:	224E779FF4D39CE90878AE3E630197E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.505770238.0000000002B01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.505770238.0000000002B01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.500003272.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.505873536.0000000002B55000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.505873536.0000000002B55000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\b2d0afa8-0593-46b1-a314-c9791c65e35d	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD01B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: vlc.exe PID: 4120 Parent PID: 3388

General

Start time:	15:51:35
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0x2c0000
File size:	248832 bytes
MD5 hash:	224E779FF4D39CE90878AE3E630197E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.314707894.00000000026E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.315101943.00000000035C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.313468004.00000000025C1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	unknown
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	6E1CC78D	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	unknown	1391	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: vlc.exe PID: 6268 Parent PID: 3388

General

Start time:	15:51:43
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0x610000
File size:	248832 bytes
MD5 hash:	224E779FF4D39CE90878AE3E630197E7
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: vlc.exe PID: 6384 Parent PID: 4120

General

Start time:	15:51:48
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x330000
File size:	248832 bytes
MD5 hash:	224E779FF4D39CE90878AE3E630197E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 6400 Parent PID: 4120

General

Start time:	15:51:49
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x6c0000
File size:	248832 bytes
MD5 hash:	224E779FF4D39CE90878AE3E630197E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.505109046.0000000002B31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.500027054.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Disassembly

Code Analysis