ID: 323839
Sample Name:
SecuriteInfo.com.Trojan.MulDrop15.61980.13868.3384
Cookbook: default.jbs
Time: 16:08:04
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

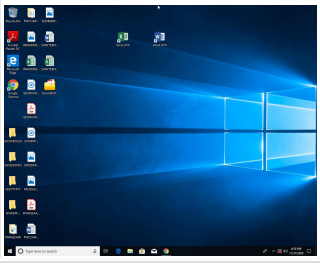
Analysis Report SecuriteInfo.com.Trojan.MulDrop15.619…

Overview

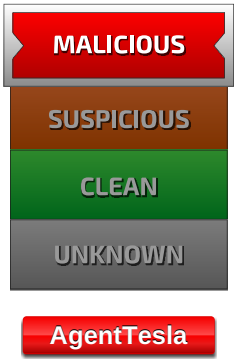
General Information

Sample Name:	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.3384 (renamed file extension from 3384 to exe)
Analysis ID:	323839
MD5:	0998148d355b1e..
SHA1:	5d062cb98564c1..
SHA256:	8ef317f2278fbe6…
Tags:	AgentTesla

Most interesting Screenshot:



Detection

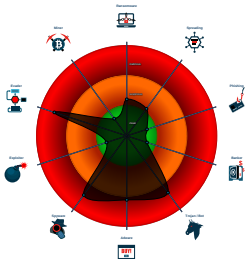


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- 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 …
- Modifies the hosts file
- 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.MulDrop15.61980.13868.exe (PID: 1740 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe' MD5: 0998148D355B1E7BAD7B44558AA4C125)
  - SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe (PID: 5936 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
  - SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe (PID: 5664 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
- vlc.exe (PID: 6248 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 0998148D355B1E7BAD7B44558AA4C125)
  - vlc.exe (PID: 6828 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
  - vlc.exe (PID: 6888 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
  - vlc.exe (PID: 6896 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
  - vlc.exe (PID: 6904 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
- vlc.exe (PID: 6536 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 0998148D355B1E7BAD7B44558AA4C125)
  - vlc.exe (PID: 6996 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "qRlQv5b8v4k0m",
  "URL: ": "http://5YdEMfw1vYcxQtIJ.com",
  "To: ": "bmmc@novget.com",
  "ByHost: ": "novget.com:587",
  "Password: ": "fTUctjBYd8i",
  "From: ": "bmmc@novget.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.301432064.0000000002C68000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.484731635.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.252302125.0000000003C61000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.301127275.0000000002BC1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 22 entries				

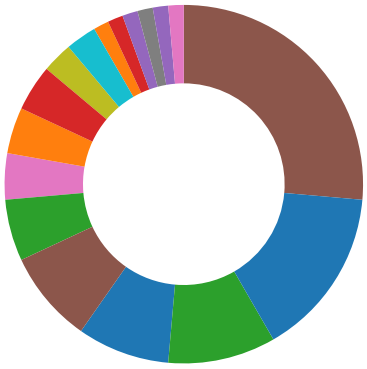
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.2.vlc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.vlc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- Spam, unwanted Advertisements and Ransom Demands
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

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

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

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

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

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:

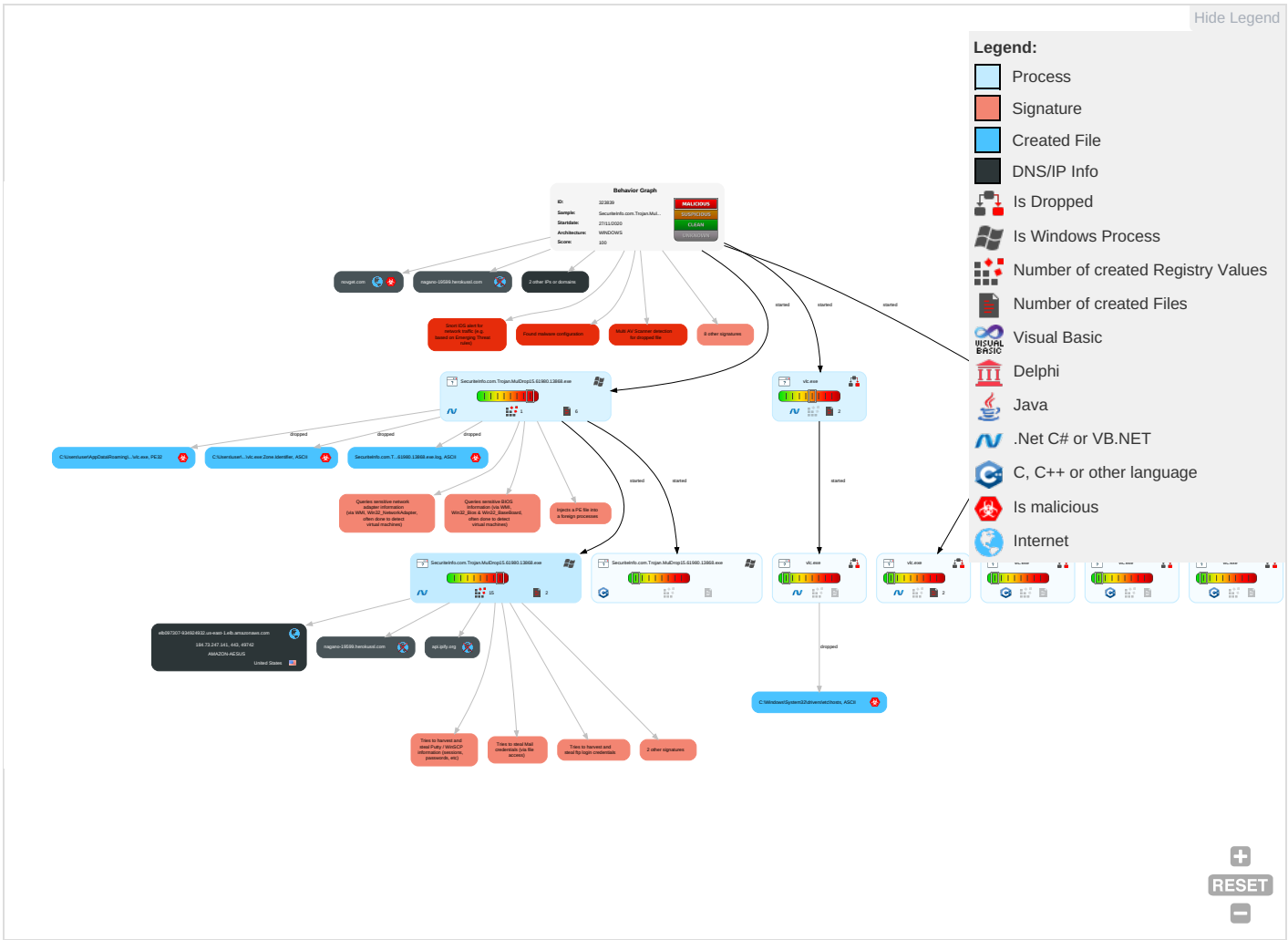
Yara detected AgentTesla

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	File and Directory Permissions Modification 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Disable or Modify Tools 1	Input Capture 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	Credentials in Registry 1	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 1	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
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
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

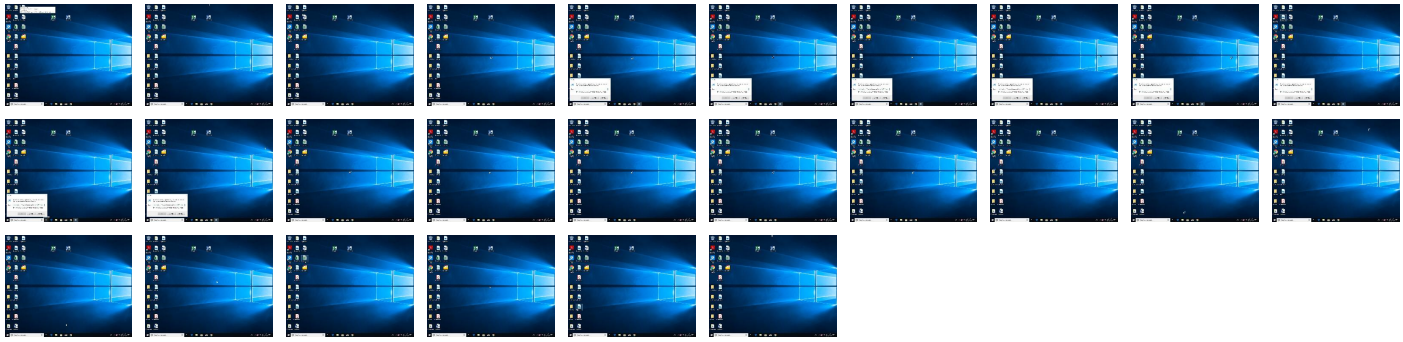
Behavior Graph



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.MulDrop15.61980.13868.exe	30%	Virustotal		Browse
SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe	31%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	
SecuriteInfo.com.Trojan.MulDrop15.61980.13868.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	31%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
20.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
novget.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.typography.netalik	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessedf	0%	Avira URL Cloud	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comditom	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.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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.sandoll.co.krU	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/r-t	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/uheT	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.carterandcone.comyrlS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Liha	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.fontbureau.comique	0%	Avira URL Cloud	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://www.jiyu-kobo.co.jp/T	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
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/N	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaT	0%	Avira URL Cloud	safe	
http://www.carterandcone.comq	0%	Avira URL Cloud	safe	
http://novget.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org4$l8	0%	Avira URL Cloud	safe	
http://5YdEMfw1vYcxQtIJ.com	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://https://discord.com/4	0%	Avira URL Cloud	safe	
http://https://discord.com/8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/m	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/l	0%	Avira URL Cloud	safe	
http://www.typography.netsiv-u	0%	Avira URL Cloud	safe	
http://HReuFq.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.comon	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitud	0%	Avira URL Cloud	safe	
http://www.typography.netez	0%	Avira URL Cloud	safe	
http://www.fontbureau.coml.TTF	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	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.founder.com.cn/cn/bThe	0%	URL Reputation	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.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.jiyu-kobo.co.jp/Y0t	0%	Avira URL Cloud	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.fontbureau.comFN	0%	Avira URL Cloud	safe	
http://www.typography.netivh	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.comcom	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	184.73.247.141	true	false		high
novget.com	167.88.170.2	true	true	• 0%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netalik	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.218827779.0000000005C2B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.491667671.0000000002FE1000.00000004.00000001.sdmp, vlc.exe, 00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comessedf	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224198483.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comalsF	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225588787.0000000005C34000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comditom	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225289437.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krU	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.219300688.0000000005C1A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/r-t	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221084547.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/uheT	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220932324.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224595210.0000000005C34000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comyrlS	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220143406.0000000005C12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Liha	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220932324.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220143406.0000000005C12000.00000004.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.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.MulDrop15.61980.13868.exe, 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.492364241.0000000003098000.00000004.00000001.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.MulDrop15.61980.13868.exe, 00000000.00000002.252302125.0000000003C61000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.484715731.0000000000402000.00000040.00000001.sdmp, vlc.exe, 00000006.00000002.301432064.0000000002C68000.00000004.00000001.sdmp, vlc.exe, 0000000B.00000002.316498806.0000000003851000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.484731635.0000000000402000.00000040.00000001.sdmp, vlc.exe, 00000014.00000002.484733374.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comique	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.223821132.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.226940473.0000000005C33000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/T	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221084547.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.491667671.0000000002FE1000.00000004.00000001.sdmp, vlc.exe, 00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/R	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221333628.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/N	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.222098114.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comaT	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.230794690.0000000005C33000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comq	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220143406.0000000005C12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/N	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.223959100.0000000005C34000.00000004.00000001.sdmp	false		high
http://novget.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.499127131.00000000034D6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org4$l8	vlc.exe, 00000013.00000002.492479441.00000000030A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://5YdEMfw1vYcxQtIJ.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.498331561.00000000348A000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.499427077.00000000034E3000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://https://discord.com/4	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/t	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221084547.0000000005C34000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.222469453.0000000005C34000.00000004.00000001.sdmp	false		unknown
http://https://discord.com/8	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/p	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220785926.0000000005C2B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/m	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221084547.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/l	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221084547.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netsiv-u	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.218760455.0000000005C2B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://HReuFq.com	vlc.exe, 00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comon	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220201223.0000000005C12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comitud	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225009614.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netez	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.218760455.0000000005C2B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comI.TTF	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225289437.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-u	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220201223.0000000005C12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersE	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224188865.0000000005C52000.00000004.00000001.sdmp	false		high
http://www.tiro.com	vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

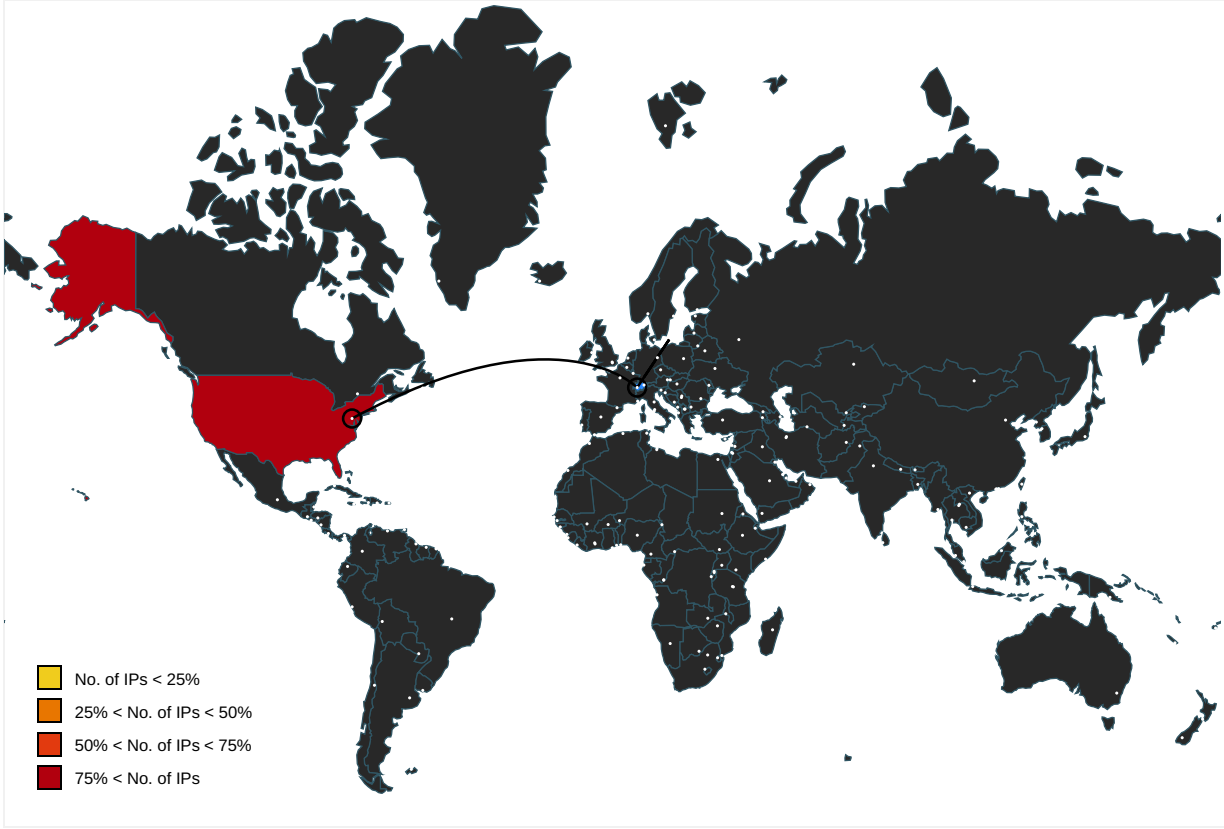
Name	Source	Malicious	Antivirus Detection	Reputation
http://elb097307-934924932.us-east-1.elb.amazonaws.com	vlc.exe, 00000013.00000002.492517745.00000000030AC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/O	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.223854426.0000000005C52000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0t	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.222098114.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220143406.0000000005C12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersP	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225123261.0000000005C52000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comFN	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224595210.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netivh	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.218760455.0000000005C2B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	vlc.exe, 00000014.00000002.492574404.0000000002E21000.00000004.00000001.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.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.492479441.00000000030A6000.00000004.00000001.sdmp	false		high
http://fontfabrik.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersk	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225457522.0000000005C52000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcom	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225487535.0000000005C34000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/m	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.222098114.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.219300688.0000000005C1A000.00000004.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comvT	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225588787.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/T	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.222098114.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersz	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224188865.0000000005C52000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cno.3	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.220143406.0000000005C12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sakkal.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.222024096.0000000005C56000.00000004.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comoitum	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.230975135.0000000005C33000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comueed	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224146770.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org/	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.492364241.0000000003098000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.492479441.00000000030A6000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225289437.0000000005C34000.00000004.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	vlc.exe, 00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wikipN	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.218382193.0000000005C30000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comtu	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224595210.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comessed7	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225289437.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comL.TTF	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.224549941.0000000005C34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.222987089.0000000005C34000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225487535.0000000005C34000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.org	vlc.exe, 00000013.00000002.492517745.00000000030AC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.0000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.neta_	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.218760455.0000000005C2B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.monotype.	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.229992289.0000000005C1B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot%telegramapi%/	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.252302125.0000000003C61000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.484715731.0000000000402000.00000040.00000001.sdmp, vlc.exe, 00000006.00000002.301432064.0000000002C68000.00000004.00000001.sdmp, vlc.exe, 0000000B.00000002.316498806.00000003851000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.484731635.0000000000402000.00000040.00000001.sdmp, vlc.exe, 00000014.00000002.484733374.0000000000402000.00000040.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221084547.0000000005C34000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.221786965.0000000005C34000.00000004.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.00000000005890000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers9	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000003.225560487.0000000005C4E000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000000.00000002.255170523.0000000005D00000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.305594390.0000000005B10000.00000002.00000001.sdmp, vlc.exe, 0000000B.00000002.320206271.00000000005890000.00000002.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.494298446.000000003325B000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.499968225.00000000067C5000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, vlc.exe, 00000013.00000002.491667671.0000000002FE1000.00000004.00000001.sdmp, vlc.exe, 00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323839
Start date:	27.11.2020
Start time:	16:08:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.3384 (renamed file extension from 3384 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:	30
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.adwa.spyw.evad.winEXE@17/7@6/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 82% • Quality standard deviation: 11%
HCA Information:	• Successful, ratio: 97% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.147.198.201, 40.88.32.150, 51.11.168.160, 23.210.248.85, 20.54.26.129, 51.104.144.132, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.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
16:09:15	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
16:09:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
16:09:29	API Interceptor	670x Sleep call for process: SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe modified
16:09:47	API Interceptor	984x Sleep call for process: vlc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.73.247.141	WeBU3HLcSGLmmDb.exe	Get hash	malicious	Browse	• api.ipify.org/
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	h5I9F5YQyX.exe	Get hash	malicious	Browse	• api.ipify.org/
	14RP4w9CuA.exe	Get hash	malicious	Browse	• api.ipify.org/
	FACTURA PENDIENTE.exe	Get hash	malicious	Browse	• api.ipify.org/
	Swift Copy_G3181992.exe	Get hash	malicious	Browse	• api.ipify.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Haruko Industrial Supply offer.exe	Get hash	malicious	Browse	• api.ipify.org/
	SKM__C20192910887888001990.pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	5fNtovgDmX.exe	Get hash	malicious	Browse	• api.ipify.org/
	1104_83924.xlsb	Get hash	malicious	Browse	• api.ipify.org/
	OZmn6gKEgi.exe	Get hash	malicious	Browse	• api.ipify.org/
	E099874321.exe	Get hash	malicious	Browse	• api.ipify.org/
	BL2648372240.xls.exe	Get hash	malicious	Browse	• api.ipify.org/
	ZAzoeb7NY6.exe	Get hash	malicious	Browse	• api.ipify.org/
	7Pkuj1axGK.exe	Get hash	malicious	Browse	• api.ipify.org/
	35pDlzhl45.exe	Get hash	malicious	Browse	• api.ipify.org/
	B3T7eh73ok.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	Payment.exe	Get hash	malicious	Browse	• api.ipify.org/
	pqE2Ika4EY.exe	Get hash	malicious	Browse	• api.ipify.org/
	QN27UyUjZ5.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
novget.com	Bjtr3wfVjY.exe	Get hash	malicious	Browse	• 167.88.170.2
	l2aaJwiUce.exe	Get hash	malicious	Browse	• 167.88.170.2
	7Z50XcJvKchMDzU.exe	Get hash	malicious	Browse	• 167.88.170.2
elb097307-934924932.us-east-1.elb.amazonaws.com	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe	Get hash	malicious	Browse	• 54.225.169.28
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	Direct Deposit.xlsx	Get hash	malicious	Browse	• 34.231.129.212
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 52.205.236.122
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 52.205.236.122
	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe	Get hash	malicious	Browse	• 54.225.169.28
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdlg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXIfrL7S45QvDvK6-2Fc04r-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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe	Get hash	malicious	Browse	• 184.73.247.141
	Purchase Order.exe	Get hash	malicious	Browse	• 184.73.247.141
	SecuriteInfo.com.Trojan.MulDrop15.61981.23282.exe	Get hash	malicious	Browse	• 184.73.247.141
	ORDER.exe	Get hash	malicious	Browse	• 184.73.247.141
	Mixtec New Order And Price List Requsting Form_pdf.exe	Get hash	malicious	Browse	• 184.73.247.141
	swift copy.exe	Get hash	malicious	Browse	• 184.73.247.141
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 184.73.247.141
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 184.73.247.141
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 184.73.247.141
	guy1.exe	Get hash	malicious	Browse	• 184.73.247.141
	guy2.exe	Get hash	malicious	Browse	• 184.73.247.141
	Exodus.exe	Get hash	malicious	Browse	• 184.73.247.141
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 184.73.247.141
	#A06578987.xlsm	Get hash	malicious	Browse	• 184.73.247.141
	Order 51897.exe	Get hash	malicious	Browse	• 184.73.247.141
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 184.73.247.141
	98650107.pdf.exe	Get hash	malicious	Browse	• 184.73.247.141
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 184.73.247.141
	Izezma64.dll	Get hash	malicious	Browse	• 184.73.247.141
	fuxenm32.dll	Get hash	malicious	Browse	• 184.73.247.141

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe.log	
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
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.MulDrop15.61980.13868.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	518656
Entropy (8bit):	7.090523037661616
Encrypted:	false
SSDEEP:	12288:5gMuIpvMHWB2naHLmFGlZ09FQFFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxc:mICE2n+jZIFqy
MD5:	0998148D355B1E7BAD7B44558AA4C125
SHA1:	5D062CB98564C1F2BC821C0A3E81B228780F77F7
SHA-256:	8EF317F2278FBE6A533E8F78B932698E986280D2F4A6716AAAAA4DC5692222A8
SHA-512:	0F824BC00379FF7F0E48C9D9E9ADFF8D38A6424B07B9E81528156747A628603E85E986DCBC618BF739FA06CCECA6343519D24C80C2B397A7887CDCAC0A0F8F3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....+._.....*.....^.... .....@.. .....@..... ..@.....K.....&..... ....H.....text...d.... ....`.rsrc....&.....(.....@..@.reloc..... .....@..B.....@.....H.....1..87.....n....h..*s.....0..t.....(....8B...8.....E....?.....8:....(... .....:....&8....*.(....8....(.... .....:....&8.....(.... ....8.....0..@..... .....8.....E...../.....8....8.... ....8....s.....8....8.... ....8.....(....r...p.....(.....(.....(.....o....t...}.... ....(....9K...& ....8@...s..... .... (....9*...&8 .....(....8]... ....8....*

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
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

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.090523037661616
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.MulDrop15.61980.13868.exe
File size:	518656
MD5:	0998148d355b1e7bad7b44558aa4c125
SHA1:	5d062cb98564c1f2bc821c0a3e81b228780f77f7
SHA256:	8ef317f2278fbe6a533e8f78b932698e986280d2f4a6716aaaaa4dc5692222a8
SHA512:	0f824bc00379ff7f0e48c9d9e9adff8d38a6424b07b9e81528156747a628603e85e986dcbc618bf739fa06cceca6343519d24c80c2b397a7887cdcac0a0f8f32
SSDEEP:	12288:5gMuIpvMHWB2naHLmFGlZ09FQFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxc:mICE2n+jZIFqy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....+._.....*.....^.... .....@.. .....@.....@.....

File Icon

Icon Hash:	d098909eaab2a282

Static PE Info

General

Entrypoint:	0x43dc5e
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:	0x5FC02BDB [Thu Nov 26 22:27:39 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3dc10	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0x426c8	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x82000	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	0x3bc64	0x3be00	False	0.969386090814	data	7.96249614821	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x3e000	0x426c8	0x42800	False	0.409991042058	data	5.87126152063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	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_ICON	0x3e4c0	0x3acd	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x41f90	0x668	data		
RT_ICON	0x425f8	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4287137928, next used block 12320655		
RT_ICON	0x428e0	0x1e8	data		
RT_ICON	0x42ac8	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x42bf0	0x662a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x4921c	0xea8	data		
RT_ICON	0x4a0c4	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 15987957, next used block 16184308		
RT_ICON	0x4a96c	0x6c8	data		
RT_ICON	0x4b034	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x4b59c	0x6014	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x515b0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 2533359616, next used block 620756992		
RT_ICON	0x61dd8	0x94a8	data		
RT_ICON	0x6b280	0x67e8	data		
RT_ICON	0x71a68	0x5488	data		
RT_ICON	0x76ef0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 16777215, next used block 520093696		
RT_ICON	0x7b118	0x25a8	data		
RT_ICON	0x7d6c0	0x10a8	data		
RT_ICON	0x7e768	0x988	data		
RT_ICON	0x7f0f0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x7f558	0x11e	data		
RT_VERSION	0x7f678	0x3f8	data		
RT_MANIFEST	0x7fa70	0xc55	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

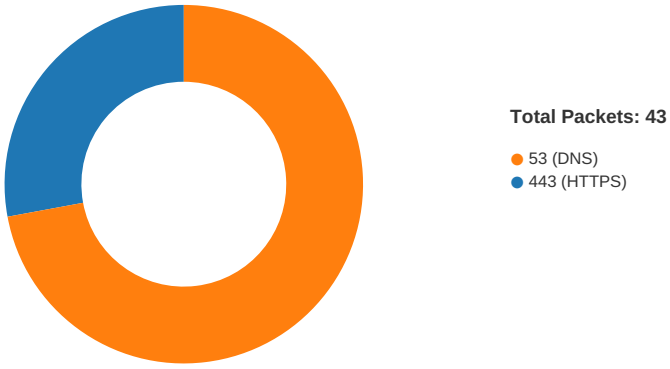
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright (c) 2020 Discord Inc. All rights reserved.
Assembly Version	0.0.52.0
InternalName	Jqeofcirr6.exe
FileVersion	0.0.52.0
CompanyName	Discord Inc.
Comments	Discord - https://discord.com/
ProductName	Discord - https://discord.com/
ProductVersion	0.0.52.0
FileDescription	Discord - https://discord.com/
OriginalFilename	Jqeofcirr6.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/27/20-16:11:05.994110	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49743	587	192.168.2.3	167.88.170.2
11/27/20-16:11:11.304820	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49745	587	192.168.2.3	167.88.170.2

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 16:10:52.158862114 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:10:52.263959885 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.264108896 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:10:52.360889912 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:10:52.463006020 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.463107109 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.463140011 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.463161945 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.463205099 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.463321924 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:10:52.463380098 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:10:52.464363098 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.501524925 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:10:52.603996038 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:52.646924973 CET	49742	443	192.168.2.3	184.73.247.141

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 16:10:52.883559942 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:10:53.026262045 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:53.222007036 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:10:53.272025108 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:11:04.340401888 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:11:04.442574024 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:11:04.442604065 CET	443	49742	184.73.247.141	192.168.2.3
Nov 27, 2020 16:11:04.442673922 CET	49742	443	192.168.2.3	184.73.247.141
Nov 27, 2020 16:11:04.442713022 CET	49742	443	192.168.2.3	184.73.247.141

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 16:08:53.528259039 CET	55984	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:53.555396080 CET	53	55984	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:54.346304893 CET	64185	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:54.373559952 CET	53	64185	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:55.077522993 CET	65110	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:55.104626894 CET	53	65110	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:55.727773905 CET	58361	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:55.754899025 CET	53	58361	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:56.383045912 CET	63492	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:56.410063982 CET	53	63492	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:57.223372936 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:57.250415087 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:58.022825956 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:58.058121920 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:58.771238089 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:58.806698084 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 16:08:59.474934101 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:08:59.501928091 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:00.408293962 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:00.435436964 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:01.230299950 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:01.257329941 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:01.880844116 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:01.908000946 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:02.573705912 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:02.600739002 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:03.226224899 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:03.265074968 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:03.861419916 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:03.888498068 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:09.480675936 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:09.516343117 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:10.691750050 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:10.718745947 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:11.561167955 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:11.596489906 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:18.477480888 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:18.504587889 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:21.647043943 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:21.685254097 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:40.545411110 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:40.588783026 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:52.954413891 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:52.981622934 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 16:09:56.917171001 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:09:56.954147100 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 16:10:28.759417057 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:10:28.786559105 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 16:10:30.345846891 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:10:30.381548882 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 16:10:51.953882933 CET	60633	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 16:10:51.980912924 CET	53	60633	8.8.8.8	192.168.2.3
Nov 27, 2020 16:10:52.011595964 CET	61292	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:10:52.038728952 CET	53	61292	8.8.8.8	192.168.2.3
Nov 27, 2020 16:11:04.332662106 CET	63619	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:11:04.384574890 CET	53	63619	8.8.8.8	192.168.2.3
Nov 27, 2020 16:11:08.244714022 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:11:08.271965027 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 16:11:08.275780916 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:11:08.303155899 CET	53	61946	8.8.8.8	192.168.2.3
Nov 27, 2020 16:11:09.849248886 CET	64910	53	192.168.2.3	8.8.8.8
Nov 27, 2020 16:11:09.884805918 CET	53	64910	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 16:10:51.953882933 CET	192.168.2.3	8.8.8.8	0x8481	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.011595964 CET	192.168.2.3	8.8.8.8	0xf6b0	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:04.332662106 CET	192.168.2.3	8.8.8.8	0xc01f	Standard query (0)	novget.com	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.244714022 CET	192.168.2.3	8.8.8.8	0xc777	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.275780916 CET	192.168.2.3	8.8.8.8	0xa647	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:09.849248886 CET	192.168.2.3	8.8.8.8	0x4321	Standard query (0)	novget.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 16:10:51.980912924 CET	8.8.8.8	192.168.2.3	0x8481	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 27, 2020 16:10:52.038728952 CET	8.8.8.8	192.168.2.3	0xf6b0	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:04.384574890 CET	8.8.8.8	192.168.2.3	0xc01f	No error (0)	novget.com		167.88.170.2	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.271965027 CET	8.8.8.8	192.168.2.3	0xc777	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:08.303155899 CET	8.8.8.8	192.168.2.3	0xa647	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 16:11:09.884805918 CET	8.8.8.8	192.168.2.3	0x4321	No error (0)	novget.com		167.88.170.2	A (IP address)	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

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 16:10:52.464363098 CET	184.73.247.141	443	192.168.2.3	49742	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	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

SecuriteInfo.com.Trojan.MulDrop15…
SecuriteInfo.com.Trojan.MulDrop15…
SecuriteInfo.com.Trojan.MulDrop15…
vlc.exe
vlc.exe
vlc.exe
vlc.exe
vlc.exe
vlc.exe
vlc.exe

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe PID: 1740
Parent PID: 5712

General

Start time:	16:08:57
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe'
Imagebase:	0x900000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
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: 00000000.00000002.252302125.0000000003C61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.252002961.0000000002C61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.252121672.0000000002D02000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	unknown
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	6CEFBEFF	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	77F42EB	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	77F42EB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\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 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 db 2b c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 0b 00 00 be 03 00 00 2a 04 00 00 00 00 00 5e dc 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 40 08 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....+._.......... ....*......^.... ....@.. ....@ ....@.................	success or wait	4	77F42EB	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	77F42EB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.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	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	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	6CEF646A	RegSetValueExW

Analysis Process: SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe PID: 5936
Parent PID: 1740

General

Start time:	16:09:12
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe
Imagebase:	0x380000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe PID: 5664
Parent PID: 1740

General

Start time:	16:09:12
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe
Imagebase:	0xdf0000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
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: 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.493762678.0000000003221000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.484715731.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.494562870.0000000003276000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6CEF1B4F	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\8a590f6c-7861-47b9-954d-45b955461a05	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CEF1B4F	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: 6248 Parent PID: 3388

General

Start time:	16:09:23
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:	0x720000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
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: 00000006.00000002.301432064.0000000002C68000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.301127275.0000000002BC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.301544638.0000000003B41000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, 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	6E0ACF06	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	6E0ACF06	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	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\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	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: vlc.exe PID: 6536 Parent PID: 3388

General

Start time:	16:09:31
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:	0x450000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
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: 0000000B.00000002.316498806.0000000003851000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.316335903.0000000002978000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: vlc.exe PID: 6828 Parent PID: 6248

General

Start time:	16:09:34
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:	0x310000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 6888 Parent PID: 6248

General

Start time:	16:09:35
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:	0x160000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 6896 Parent PID: 6248

General

Start time:	16:09:36
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:	0x210000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 6904 Parent PID: 6248

General

Start time:	16:09:36
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:	0xa30000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
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: 00000013.00000002.484731635.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.491667671.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.491667671.0000000002FE1000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6CEF1B4F	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: vlc.exe PID: 6996 Parent PID: 6536

General

Start time:	16:09:43
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:	0x870000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
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: 00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.492574404.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.484733374.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis