ID: 323672
Sample Name:
SecuriteInfo.com.Trojan.Siggen11.49316.15393.7982
Cookbook: default.jbs
Time: 10:41:26
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

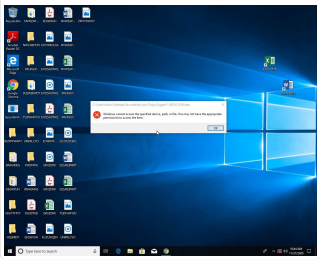
Analysis Report SecuriteInfo.com.Trojan.Siggen11.4931…

Overview

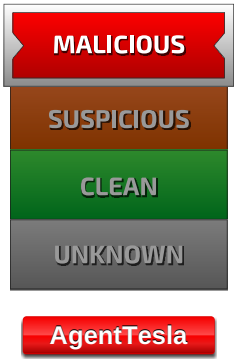
General Information

Sample Name:	SecuriteInfo.com.Trojan.Siggen11.49316.15393.7982 (renamed file extension from 7982 to exe)
Analysis ID:	323672
MD5:	9817218c055db1..
SHA1:	c5233c8d5a0973..
SHA256:	ba41a55277d319..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

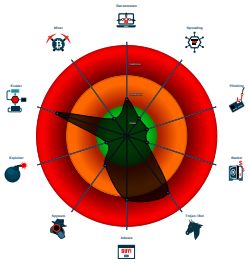


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Adds a directory exclusion to Windo…
- Connects to a pastebin service (like…
- Creates an undocumented autostart …
- Creates autostart registry keys with …
- Creates multiple autostart registry ke…
- Drops PE files to the startup folder
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe (PID: 5940 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' MD5: 9817218C055DB1B75D64DF2AE2F40F53)
  - powershell.exe (PID: 6204 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6236 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6292 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6356 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe (PID: 6700 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe MD5: 9817218C055DB1B75D64DF2AE2F40F53)
- SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe (PID: 6816 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' MD5: 9817218C055DB1B75D64DF2AE2F40F53)
- SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe (PID: 7112 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' MD5: 9817218C055DB1B75D64DF2AE2F40F53)
- SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe (PID: 4864 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' MD5: 9817218C055DB1B75D64DF2AE2F40F53)
- SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe (PID: 1308 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' MD5: 9817218C055DB1B75D64DF2AE2F40F53)
- SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe (PID: 1460 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' MD5: 9817218C055DB1B75D64DF2AE2F40F53)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.578444505.000000000371 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000012.00000002.510166428.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: SecuriteInfo.com.Trojan.Sigg en11.49316.15393.exe PID: 6700	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: SecuriteInfo.com.Trojan.Sigg en11.49316.15393.exe PID: 6700	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

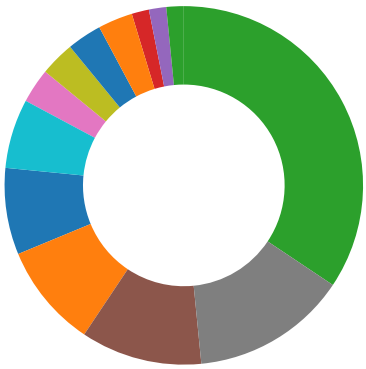
Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.SecuriteInfo.com.Trojan.Siggen11.49316.15393. exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

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:

Connects to a pastebin service (likely for C&C)

Boot Survival:

Creates an undocumented autostart registry key

Creates autostart registry keys with suspicious names

Creates multiple autostart registry keys

Drops PE files to the startup folder

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)

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

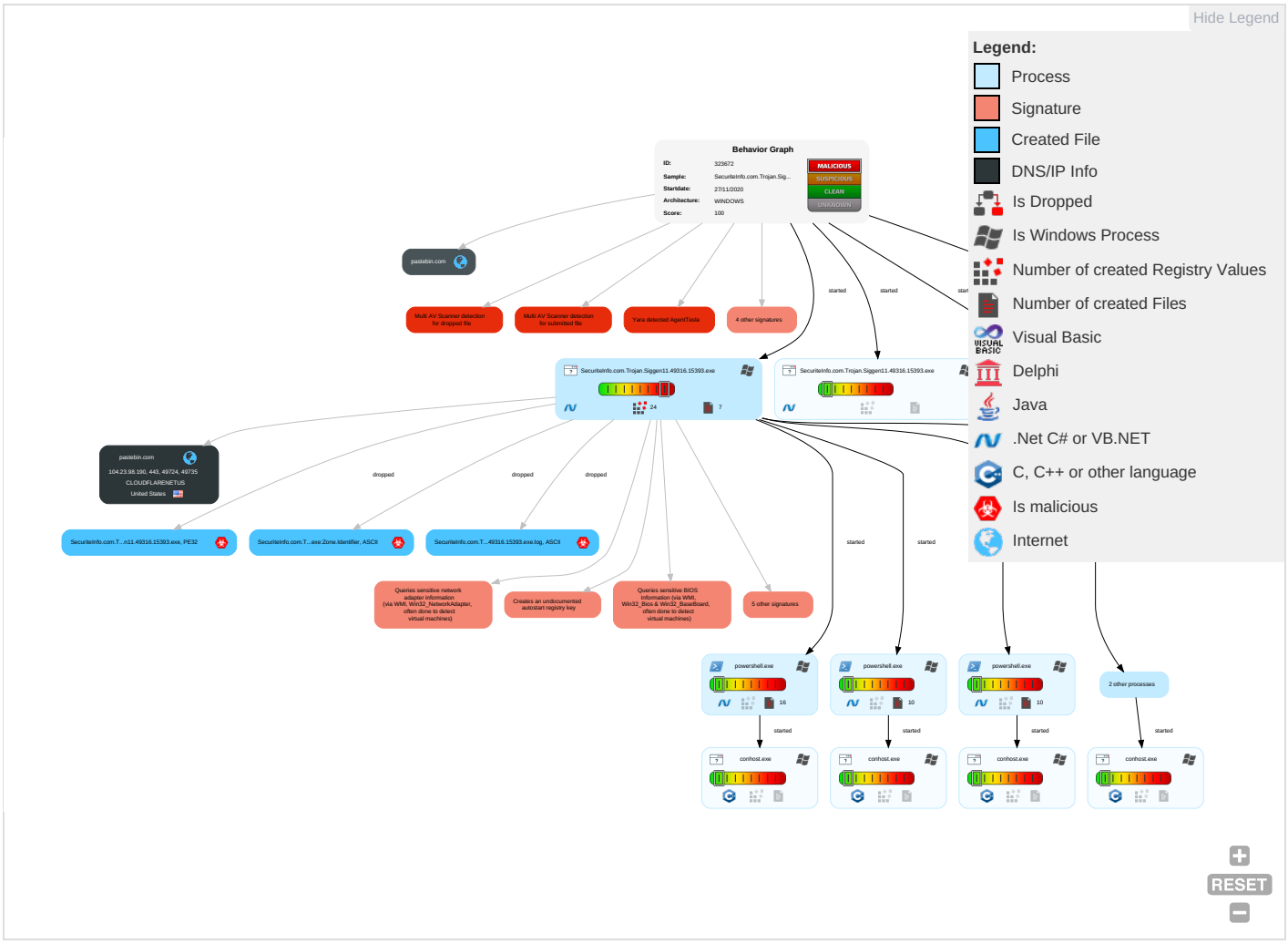
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Startup Items 1	Startup Items 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 4 2 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 1 4	LSASS Memory	Security Software Discovery 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 4 2 1	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

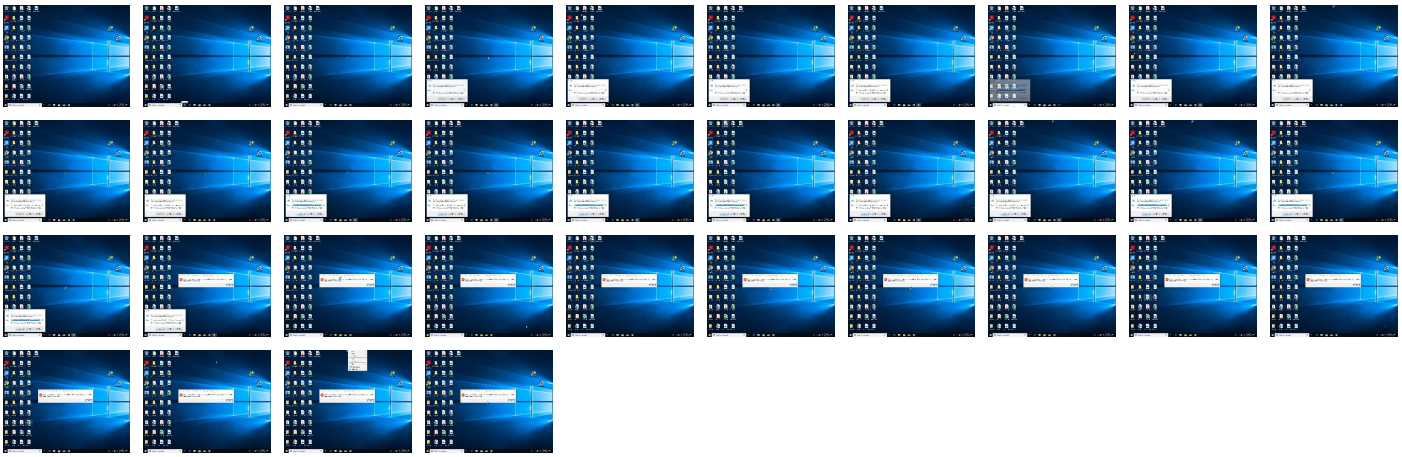
Behavior Graph

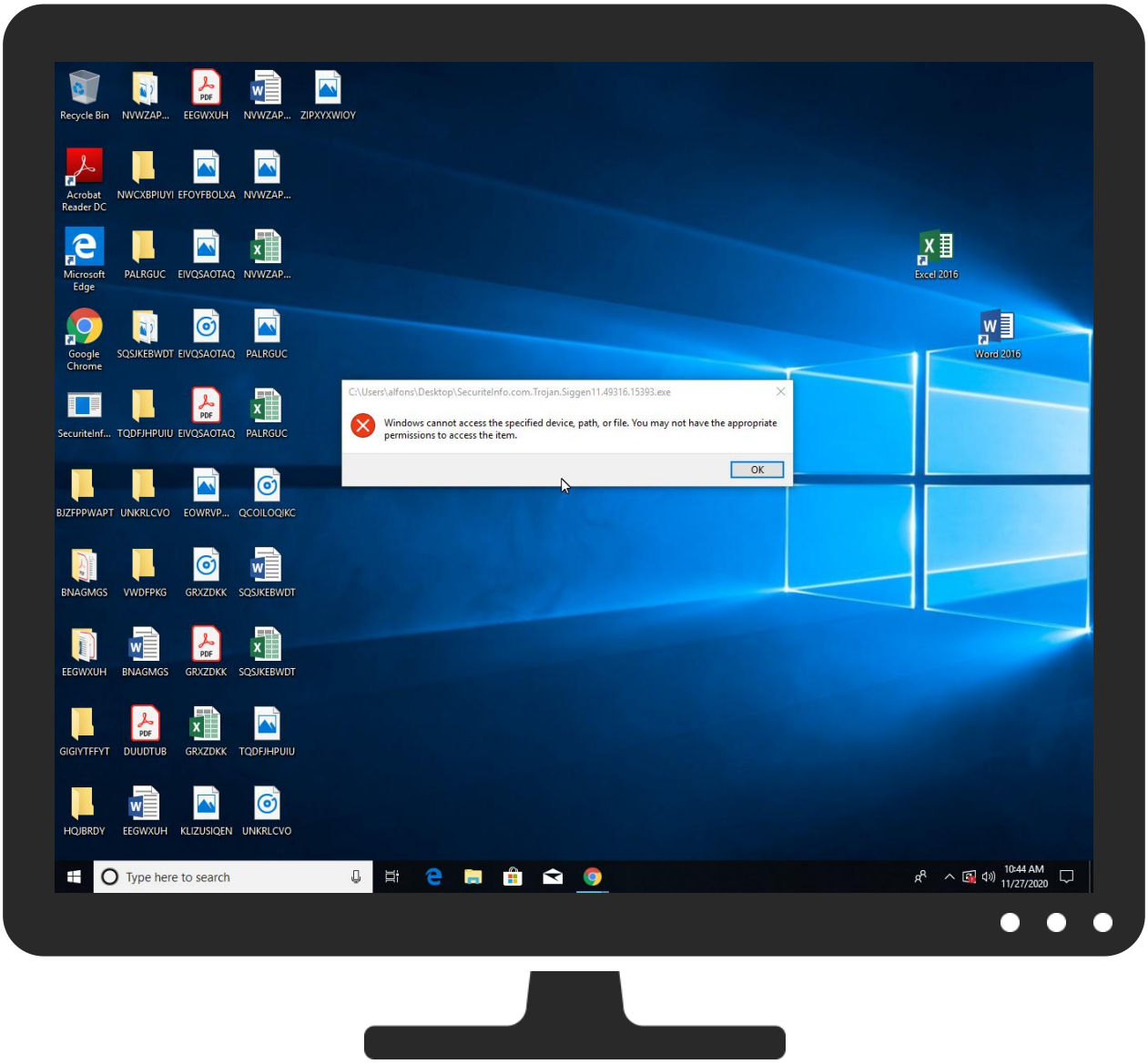


Screenshots

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.Siggen11.49316.15393.exe	38%	Virustotal		Browse
SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	14%	Metadefender		Browse
SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Vimditator	
SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	38%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Vimditator	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gypycQ.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://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	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://pesterbdd.com/images/Pester.png8	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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

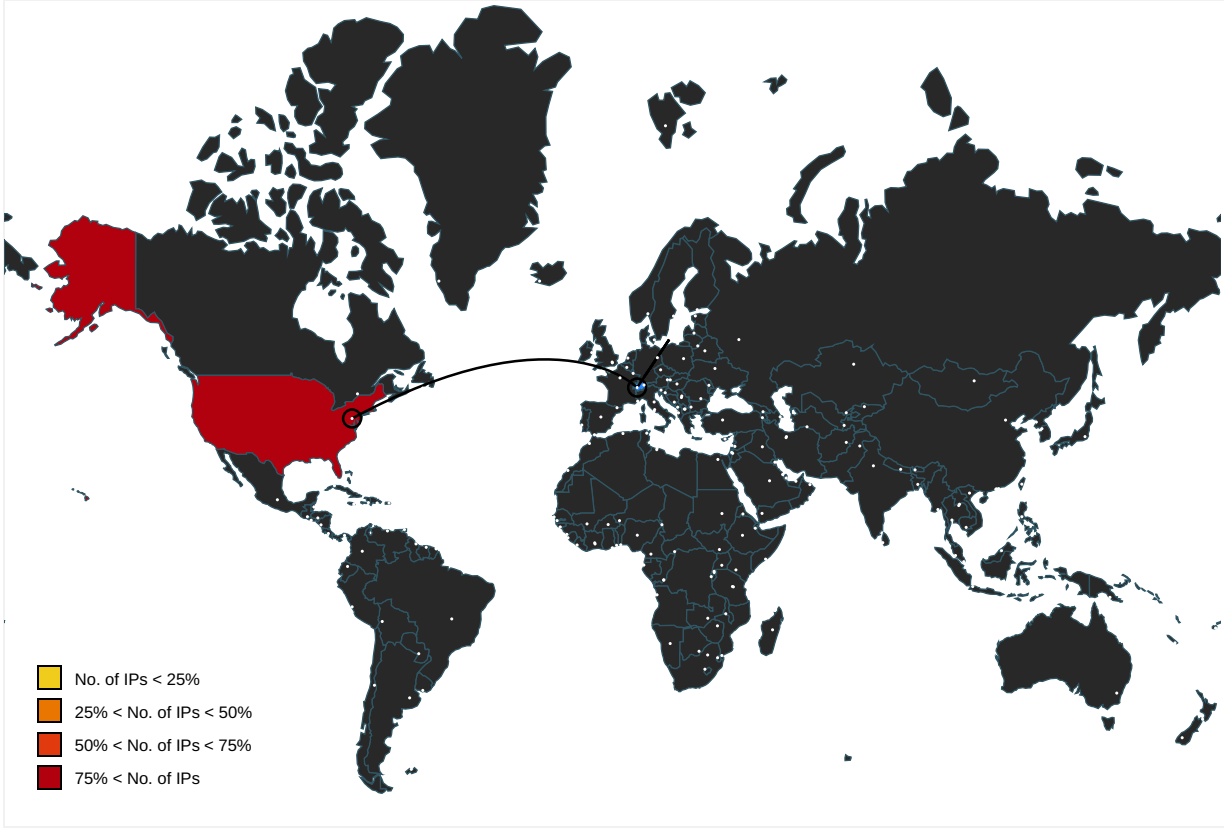
Name	IP	Active	Malicious	Antivirus Detection	Reputation
pastebin.com	104.23.98.190	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://gypycQ.com	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe, 00000012.00000002.578444505.0000000003711000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe, 00000012.00000002.578444505.0000000003711000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	low
http://DynDns.comDynDNS	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe, 00000012.00000002.578444505.0000000003711000.00000004.00000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	unknown
http://crl.m	powershell.exe, 00000009.00000003.472140307.0000000007945000.00000004.00000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000010.00000002.575593702.0000000004A80000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000009.00000002.581579204.000000000492E000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.584317147.00000000045C2000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.583300730.000000004D7E000.00000004.00000001.sdmp, powershell.exe, 00000010.00000002.575593702.0000000004A80000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe, 00000012.00000002.578444505.0000000003711000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000010.00000002.575593702.0000000004A80000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe, 00000012.00000002.510166428.0000000000402000.00000040.00000001.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000009.00000002.581579204.000000000492E000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.584317147.00000000045C2000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.583300730.000000004D7E000.00000004.00000001.sdmp, powershell.exe, 00000010.00000002.575593702.0000000004A80000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000009.00000002.571999059.00000000047F1000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.582959896.0000000004481000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.576001862.000000004C41000.00000004.00000001.sdmp, powershell.exe, 00000010.00000002.568242550.0000000004941000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe, 00000012.00000002.578444505.0000000003711000.00000004.00000001.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.Siggen11.49316.15393.exe, 00000012.00000002.510166428.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000010.00000002.575593702.0000000004A80000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png8	powershell.exe, 0000000C.00000002.584317147.00000000045C2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester8	powershell.exe, 0000000C.00000002.584317147.00000000045C2000.00000004.00000001.sdmp	false		high
http://https://api.ipify.orgGETMozilla/5.0	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe, 00000012.00000002.578444505.0000000003711000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html8	powershell.exe, 0000000C.00000002.584317147.00000000045C2000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.23.98.190	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323672
Start date:	27.11.2020
Start time:	10:41:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Siggen11.49316.15393.7982 (renamed file extension from 7982 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:	31
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.evad.winEXE@20/18@4/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 23.210.248.85, 51.104.139.180, 20.54.26.129, 51.103.5.159, 92.122.213.194, 92.122.213.247, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net • 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
10:43:00	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
10:43:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
10:43:13	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe modified
10:43:19	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
10:43:28	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
10:43:38	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
10:43:59	API Interceptor	116x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.23.98.190	b095b966805abb7df4ffddf183def880.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	E1Q0TjeN32.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	6YCl3ATKJw.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	Hjnb15Nuc3.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	JDgYMW0LHW.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	4av8Sn32by.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	5T4Ykc0VSK.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	afvhKak0Ir.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	T6OcyQsUsY.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	1KITgJnGbI.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PxwWcmbMC5.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	XnAJZR4NcN.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PbTwrajNMX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	22NO7gVJ7r.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	rE7DwszvrX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VjPHSJkwr6.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	wf86K0dpOP.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VrR9J0FnSG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	6C1MYmrVl1.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	aTZQZVVriQ.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pastebin.com	SecuriteInfo.com.Trojan.Nanocore.23.20965.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.VirRansom.rm.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.Trojan.KillProc2.14740.25300.exe	Get hash	malicious	Browse	• 104.23.99.190
	due-invoice.xlsm	Get hash	malicious	Browse	• 104.23.98.190
	Order 51897.exe	Get hash	malicious	Browse	• 104.23.99.190
	Statement Of Account.exe	Get hash	malicious	Browse	• 104.23.98.190
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 104.23.98.190
	BTNCRKWd.exe	Get hash	malicious	Browse	• 104.23.98.190
	Shipment Details.exe	Get hash	malicious	Browse	• 104.23.98.190
	7iZX0KCH4C.exe	Get hash	malicious	Browse	• 104.23.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IFEvMPuK1t.exe	Get hash	malicious	Browse	• 104.23.98.190
	lzh-content.exe	Get hash	malicious	Browse	• 104.23.98.190
	New Order.exe	Get hash	malicious	Browse	• 104.23.98.190
	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	BT2wDapfoI.exe	Get hash	malicious	Browse	• 104.23.98.190
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	ShippingDoc.jar	Get hash	malicious	Browse	• 104.23.98.190
	a66a5257bb6ee2e690450c48a91815d4.exe	Get hash	malicious	Browse	• 104.23.99.190

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Re.Po ORDER.45355.SCAN.PDF...exe	Get hash	malicious	Browse	• 104.28.5.151
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 172.67.212.166
	lxpo.exe	Get hash	malicious	Browse	• 162.159.128.233
	SpecificationX20202611.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	SecuriteInfo.com.Trojan.Nanocore.23.20965.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 172.67.143.180
	trackinginfo#U007eupdate.jar	Get hash	malicious	Browse	• 104.20.23.46
	trackinginfo#U007eupdate.jar	Get hash	malicious	Browse	• 104.20.22.46
	MAL.PPT	Get hash	malicious	Browse	• 172.67.219.133
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 104.16.18.94
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 104.27.146.211
	SecuriteInfo.com.BehavesLike.Win32.VirRansom.rm.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.Trojan.KillProc2.14740.25300.exe	Get hash	malicious	Browse	• 104.23.99.190
	http://https://rb.gy/flx7ju	Get hash	malicious	Browse	• 104.28.9.39
	http://https://bit.ly/3kUgQ0H	Get hash	malicious	Browse	• 172.67.131.94
	EME_PO.47563.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Shipping documents.xlsx	Get hash	malicious	Browse	• 104.16.16.194
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 162.159.138.81
	Nota di consegna_TNT507CC.exe	Get hash	malicious	Browse	• 104.18.54.93
	txema_inef_post_live_loader_88.exe	Get hash	malicious	Browse	• 104.18.35.76

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Re.Po ORDER.45355.SCAN.PDF...exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Trojan.Nanocore.23.20965.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.VirRansom.rm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Trojan.KillProc2.14740.25300.exe	Get hash	malicious	Browse	• 104.23.98.190
	txema_inef_post_live_loader_88.exe	Get hash	malicious	Browse	• 104.23.98.190
	QQWUO898519.xls	Get hash	malicious	Browse	• 104.23.98.190
	Purchase Order 5654.Scan.pdf...exe	Get hash	malicious	Browse	• 104.23.98.190
	BTNCRKWd.exe	Get hash	malicious	Browse	• 104.23.98.190
	IRS NOTICE LETTER.exe	Get hash	malicious	Browse	• 104.23.98.190
	Shipment Details.exe	Get hash	malicious	Browse	• 104.23.98.190
	IFEvMPuK1t.exe	Get hash	malicious	Browse	• 104.23.98.190
	out.exe	Get hash	malicious	Browse	• 104.23.98.190
	lzh-content.exe	Get hash	malicious	Browse	• 104.23.98.190
	Unconfirmed 384649.exe	Get hash	malicious	Browse	• 104.23.98.190
	invoice_no_H04618.doc	Get hash	malicious	Browse	• 104.23.98.190
	New Order.exe	Get hash	malicious	Browse	• 104.23.98.190
	MV TBN.exe	Get hash	malicious	Browse	• 104.23.98.190

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHY
MD5:	45A1687CECD48F6A4A90071C96E50E41
SHA1:	DF49ED05380F17EB14F2B87F051676E8B681E7E2
SHA-256:	05DABE990DCB3015952FAA3AE9AD3E43F70FF3BDB2E17E3B7A183CBDCDAF7C49
SHA-512:	1E0683F03744B715EC699179412C4E1BF44ED1D98F4ACE22366FB860773C8FF6A02D809BCAA1170BDD712B94A3FFBB9990ED0E9BD494E4622E37D3A5CDED33 B
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	698
Entropy (8bit):	5.049094101509586
Encrypted:	false
SSDEEP:	12:reVGyMYx2Y5BYtmWNUc5AtYX5E4a2KryMYGH+ptsxptsOtw9O9S8:reUyMGF5ytmLcetYX5E2KryMb+zsxzsk
MD5:	B0CEEA53B3467F59FD8E87F80213BDE9
SHA1:	D9E6D1CBB480E7248658DF935648DFA733745602
SHA-256:	D9C93CB64E6F1F5BDC94581CEEA99F759EE1E35716EAF623C61962EA0152F9DD
SHA-512:	DDAA6C9FA3535B4926C60B692F8E202D10EB160D1F8BE7A9DE79239EF75AFD470403DF1D8F0CBF29A5F819E907D02E8E656BB9A52E71E30D9259987EAE88165 5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D..8.....C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation..... ..Invoke-OperationValidation.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3i44lw5f.d2x.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_divrs4p2.qmp.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_f3yslelb.mfk.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_j0cgkrpy.lx1.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m2jlipkf.1y1.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mufbm2g2.2lz.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xk5gz5yj.lnm.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_z5ws434f.y2b.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	10985472
Entropy (8bit):	5.35336221586183
Encrypted:	false
SSDEEP:	98304:f8Ysop+DEE0tLMVJfQXMjGKY+uyflLm1jFcIdxR9cy6VNsFm3rN9Yb/xy5AISV7F:f8aPMo+uOKILXE
MD5:	9817218C055DB1B75D64DF2AE2F40F53
SHA1:	C5233C8D5A0973A76186707337A952A73C02B07E
SHA-256:	BA41A55277D31931DED743F6D9A984D0A22E7F6C79F753DA9493929D1942CBC8
SHA-512:	29C6502A1813A41FB37B6B35347059179F309F673CA78C818E91C65BDD8AA2CDB78FB5E398562BA2D5AF4AB8215017D3477CB650107A36A70761F2AE2C6FB523
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 38%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 29%

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?~._.....N.... .....@.. ..... .@.....W..... ....H.....text...T.... ....`.reloc.....@..B..... .....0.....H.....".....*.... ....@..... ....ro..p(....*.....r...p(....*. ....*....90...(....9.....rG..p....(....(...*.....(!...*....*...~ ....: ...r...p.....(....o....s%.....~.....o&...*..('...*....0..... ....(.....~....(....&....8.....* ....*(.... ....(....(... ....* ....** ....* ....* ....*~....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.+lqbRRN1.20201127104302.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	5.33438609984993
Encrypted:	false
SSDEEP:	24:BxSAzDvBB5x2DOXUWeSuvuVM4JL8W+aHjeTKKjX4CIym1ZJXauvuVM4JLY:BZ/v/5oO+SsuHJLH+aqDYB1ZAsuHJLY
MD5:	25A2CB966C1BC855223E5FE331C76C11
SHA1:	7C8D65DDB351557447A4B0F6D56343C5528D8F2E
SHA-256:	6DDD5C49FB8F2C51994A1EFE3B3842CBC045DF65EAEBDF23D865FC9326BFCC46
SHA-512:	73CCE6F6E5E18B0412C8FEFD8753EBCC8028B01FD2C8E55BCC4D27EAF63D80E16874EA58C423823769B4A0FFB07267047A15AEEE9548472ADB3EC56E829529 C
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201127104335..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe -Force..Process ID: 6292..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201127104338..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.E60ONHS3.20201127104300.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	5.328914347811565
Encrypted:	false
SSDEEP:	24:BxSADDvBB5x2DOXUWeSuvuVM4JL8WoaHjeTKKjX4CIym1ZJXpNuvuVM4JLY:BZPv/5oO+SsuHJLH3qDYB1ZzNsuHJLY
MD5:	454F4C753655885711BF44A81F9F27B1
SHA1:	E1ED0450C5FBC149BD1371DA4E407BFA32E1927E
SHA-256:	98762BA8AB1FFE47DBE44D0E36DB525329AD38B7DC7724AA9DEF291CA9E73040
SHA-512:	CACA1899327BF27508BFE8E08526B11999504ECC7CCEE02DBE061B6146A70311E632ED7C677160F42FFCE6B35FE1AD435419C2B5D74907BF856AAB1091D68BE 8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201127104340..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe -Force..Process ID: 6236..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201127104340..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.VosWW7ND.20201127104259.txt

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.VosWW7ND.20201127104259.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	5.3331410794166505
Encrypted:	false
SSDEEP:	24:BxSA9DvBB5x2DOXUWeSuvuVM4JL8W4HjeTKKjX4CIym1ZJXqduvuVM4JLY:BZFv/5oO+SsuHJLH4qDYB1Z4dsuHJLY
MD5:	7F1706C1ED2F3D3DEF39D8EF52F6FF45
SHA1:	1329654BE293F4B7EB2F70A3C65C4ADC0A4107E7
SHA-256:	5A3457A9CAE95AC2DFE7D3150677F90AF9BA17AC6522BA7ED0B885FD0D7162F9
SHA-512:	D769C98D133E2D88BA0F9C490E21ABA1D5677E54AAF9CAFDA7208A74BAB7F254D4DF84D30D311FA20B24E48CDF01DCC93502A983CE0326D02E02B2A096780E46
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201127104328..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe -Force..Process ID: 6204..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201127104329..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.e7cWhL8o.20201127104302.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.3192412929516735
Encrypted:	false
SSDEEP:	24:BxSAUyDvBB5x2DOXUWeSuVaJL8W4HjeTKKjX4CIym1ZJXbNuVaJLY:BZbv/5oO+SmaJLH4qDYB1ZXmaJLY
MD5:	89B79C7A33CA9878680E79C88AC4D1CE
SHA1:	78FF0F3923D877953238599BDE3DDD3D084F6BE2
SHA-256:	297A20BDDB6F21DA7427004F7C11D710A883047377A3FF8920D6B5D8EDDC1EB2
SHA-512:	6957B81BD5A4A7B92A4B869F84F58DF969592871D3111AD1FB5B44A01F07FDCA0684B7838B0B1C770BC096A469E6F9EDDA663038179C1F9E13DC99F0F5CE3FE
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201127104344..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe -Force..Process ID: 6356..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201127104346..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe -Force..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.35336221586183
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
File size:	10985472
MD5:	9817218c055db1b75d64df2ae2f40f53
SHA1:	c5233c8d5a0973a76186707337a952a73c02b07e
SHA256:	ba41a55277d31931ded743f6d9a984d0a22e7f6c79f753da9493929d1942cbc8
SHA512:	29c6502a1813a41fb37b6b35347059179f309f673ca78c818e91c65bdd8aa2cdb78fb5e398562ba2d5af4ab8215017d3477cb650107a36a70761f2ae2c6fb523
SSDEEP:	98304:f8Ysop+DEE0tLMVJfQXMjGKY+uyflLm1jFcIdxR9cy6VNsFm3rN9Yb/xy5AISV7F:f8aPMo+uOKILXE

General

File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L...? ~._............................N.... ....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0xe7bb4e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBF7E3F [Thu Nov 26 10:06:55 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa7baf4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa7c000	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

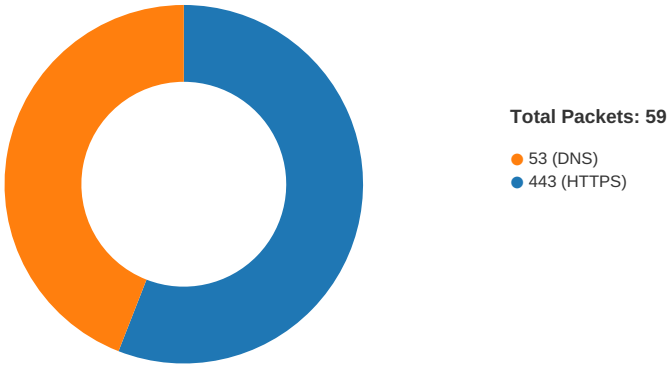
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa79b54	0xa79c00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xa7c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 10:42:49.210939884 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:42:49.227663994 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.228703022 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:42:49.316282034 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:42:49.332832098 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.337892056 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.337918997 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.337929964 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.337992907 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:42:49.343219995 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:42:49.359678030 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.359776020 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.402453899 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:42:49.468096972 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:42:49.484747887 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.783586979 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.783612967 CET	443	49724	104.23.98.190	192.168.2.5
Nov 27, 2020 10:42:49.783709049 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:43:02.762116909 CET	49724	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:28.208461046 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:28.225073099 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.225209951 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:28.233000994 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:28.249475956 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.254827023 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.254853964 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.254869938 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.254930019 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:28.257344007 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:28.273796082 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.273998976 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.304749966 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:28.321326971 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.331960917 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.331984043 CET	443	49735	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:28.332086086 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.063083887 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.079790115 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.079941034 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.083087921 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.099596977 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.102190971 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.102226973 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.102243900 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.102278948 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.104842901 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.121294975 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.138658047 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.144655943 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.161896944 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.184834957 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.184859991 CET	443	49736	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.184995890 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.402369022 CET	49737	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.419006109 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.419123888 CET	49737	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.422456026 CET	49737	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.439008951 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.444595098 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.444621086 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.444638014 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.444749117 CET	49737	443	192.168.2.5	104.23.98.190

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 10:44:29.446398973 CET	49737	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.462999105 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.463185072 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.491647959 CET	49737	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:29.508317947 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.525293112 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.525322914 CET	443	49737	104.23.98.190	192.168.2.5
Nov 27, 2020 10:44:29.525441885 CET	49737	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:31.432687044 CET	49735	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:33.924727917 CET	49736	443	192.168.2.5	104.23.98.190
Nov 27, 2020 10:44:35.577064991 CET	49737	443	192.168.2.5	104.23.98.190

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 10:42:13.336673975 CET	63183	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:13.372376919 CET	53	63183	8.8.8.8	192.168.2.5
Nov 27, 2020 10:42:13.989336967 CET	60151	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:14.016511917 CET	53	60151	8.8.8.8	192.168.2.5
Nov 27, 2020 10:42:15.059585094 CET	56969	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:15.086910963 CET	53	56969	8.8.8.8	192.168.2.5
Nov 27, 2020 10:42:16.186050892 CET	55161	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:16.213366985 CET	53	55161	8.8.8.8	192.168.2.5
Nov 27, 2020 10:42:17.316363096 CET	54757	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:17.343581915 CET	53	54757	8.8.8.8	192.168.2.5
Nov 27, 2020 10:42:35.866643906 CET	49992	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:36.414371967 CET	53	49992	8.8.8.8	192.168.2.5
Nov 27, 2020 10:42:37.587930918 CET	60075	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:37.615092993 CET	53	60075	8.8.8.8	192.168.2.5
Nov 27, 2020 10:42:49.072839022 CET	55016	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:42:49.108422041 CET	53	55016	8.8.8.8	192.168.2.5
Nov 27, 2020 10:43:01.681854010 CET	64345	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:43:01.725712061 CET	53	64345	8.8.8.8	192.168.2.5
Nov 27, 2020 10:43:02.039285898 CET	57128	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:43:02.077198029 CET	53	57128	8.8.8.8	192.168.2.5
Nov 27, 2020 10:43:11.716787100 CET	54791	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:43:11.752753019 CET	53	54791	8.8.8.8	192.168.2.5
Nov 27, 2020 10:43:43.003576040 CET	50463	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:43:43.030673981 CET	53	50463	8.8.8.8	192.168.2.5
Nov 27, 2020 10:43:53.252940893 CET	50394	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:43:53.288631916 CET	53	50394	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:28.096323013 CET	58530	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:28.131696939 CET	53	58530	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:28.946517944 CET	53813	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:28.982189894 CET	53	53813	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:29.236959934 CET	63732	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:29.272761106 CET	53	63732	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:52.928201914 CET	57344	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:53.007874966 CET	53	57344	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:53.338449955 CET	54450	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:53.374043941 CET	53	54450	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:53.725214005 CET	59261	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:53.762211084 CET	53	59261	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:54.316193104 CET	57151	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:54.351866961 CET	53	57151	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:54.612435102 CET	59413	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:54.649458885 CET	53	59413	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:54.941310883 CET	60516	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:54.976882935 CET	53	60516	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:55.278824091 CET	51649	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:55.314621925 CET	53	51649	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:55.696048975 CET	65086	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:55.731633902 CET	53	65086	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:56.169977903 CET	56432	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 10:44:56.205749035 CET	53	56432	8.8.8.8	192.168.2.5
Nov 27, 2020 10:44:56.477191925 CET	52929	53	192.168.2.5	8.8.8.8
Nov 27, 2020 10:44:56.516211033 CET	53	52929	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 10:42:49.072839022 CET	192.168.2.5	8.8.8.8	0xc51d	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:28.096323013 CET	192.168.2.5	8.8.8.8	0xacdc	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:28.946517944 CET	192.168.2.5	8.8.8.8	0x6a3c	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:29.236959934 CET	192.168.2.5	8.8.8.8	0x65a	Standard query (0)	pastebin.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 10:42:49.108422041 CET	8.8.8.8	192.168.2.5	0xc51d	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 27, 2020 10:42:49.108422041 CET	8.8.8.8	192.168.2.5	0xc51d	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:28.131696939 CET	8.8.8.8	192.168.2.5	0xacdc	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:28.131696939 CET	8.8.8.8	192.168.2.5	0xacdc	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:28.982189894 CET	8.8.8.8	192.168.2.5	0x6a3c	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:28.982189894 CET	8.8.8.8	192.168.2.5	0x6a3c	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:29.272761106 CET	8.8.8.8	192.168.2.5	0x65a	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 27, 2020 10:44:29.272761106 CET	8.8.8.8	192.168.2.5	0x65a	No error (0)	pastebin.com		104.23.99.190	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
Nov 27, 2020 10:42:49.337929964 CET	104.23.98.190	443	192.168.2.5	49724	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 27, 2020 10:44:28.254869938 CET	104.23.98.190	443	192.168.2.5	49735	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

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 10:44:29.102243900 CET	104.23.98.190	443	192.168.2.5	49736	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020 Mon Jan 27 13:46:39 CET 2020	Tue Aug 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 27, 2020 10:44:29.444638014 CET	104.23.98.190	443	192.168.2.5	49737	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020 Mon Jan 27 13:46:39 CET 2020	Tue Aug 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

- SecuriteInfo.com.Trojan.Siggen11.4..
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- SecuriteInfo.com.Trojan.Siggen11.4..
- SecuriteInfo.com.Trojan.Siggen11.4..
- SecuriteInfo.com.Trojan.Siggen11.4..
- SecuriteInfo.com.Trojan.Siggen11.4..
- SecuriteInfo.com.Trojan.Siggen11.4..
- SecuriteInfo.com.Trojan.Siggen11.4..

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe PID: 5940
Parent PID: 5724

General

Start time:	10:42:30
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe'
Imagebase:	0x450000
File size:	10985472 bytes
MD5 hash:	9817218C055DB1B75D64DF2AE2F40F53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB0CF06	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	6DB0CF06	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.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	6C95DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C95DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\59100918-590d-458f-8202-b1bfda19b584	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C95BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE1C78D	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\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	0	1048576	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 3f 7e bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 9c a7 00 00 02 00 00 00 00 00 00 4e bb a7 00 00 20 00 00 00 c0 a7 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 e0 a7 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...? ~._............................N.... ....@.. ....@.................	success or wait	11	6C95DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.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	6C95DD66	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe.log	unknown	1216	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DE1C907	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	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	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	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C951B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6C955F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6C955F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6C955F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6C955F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6C955F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6C955F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	<Unknown>	unicode	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	success or wait	1	6C95646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	dword	0	success or wait	1	6C95C075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	shell	unicode	explorer.exe,"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe"	success or wait	1	6C95646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	unicode	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	success or wait	1	6C95646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	dword	0	success or wait	1	6C95C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6C95C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6C95C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6C95C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6C95C075	RegSetValueExW

Analysis Process: powershell.exe PID: 6204 Parent PID: 5940

General

Start time:	10:42:57
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force
Imagebase:	0x910000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB0CF06	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	6DB0CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8B5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8B5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2jlipkf.1y1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j0cgkrpy.lx1.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\Documents\20201127	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C95BEFF	CreateDirectoryW
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.VosWW7ND.20201127104259.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2jlipkf.1y1.ps1	success or wait	1	6C956A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j0cgkrpy.lx1.psm1	success or wait	1	6C956A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2jlipkf.1y1.ps1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j0cgkrpy.lx1.psm1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.VosWW7ND.20201127104259.txt	unknown	3	ef bb bf	...	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.VosWW7ND.20201127104259.txt	unknown	767	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 37 31 30 34 33 32 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 39 32 32 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201127104328..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6C951B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....w.e....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6C951B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DAF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	123	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4\9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C951B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C951B4F	ReadFile

Analysis Process: conhost.exe PID: 6228 Parent PID: 6204

General

Start time:	10:42:57
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6236 Parent PID: 5940

General

Start time:	10:42:57
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force
Imagebase:	0x910000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB0CF06	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	6DB0CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8B5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8B5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3i44lw5f.d2x.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_divrs4p2.qmp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.E60ONHS3.20201127104300.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3i44lw5f.d2x.ps1	success or wait	1	6C956A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_divrs4p2.qmp.psm1	success or wait	1	6C956A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3i44lw5f.d2x.ps1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_divrs4p2.qmp.psm1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.E60ONHS3.20201127104300.txt	unknown	3	ef bb bf	...	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.E60ONHS3.20201127104300.txt	unknown	767	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 37 31 30 34 33 34 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 39 32 32 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201127104340..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6C951B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....w.e....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6C951B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DAF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C951B4F	ReadFile

Analysis Process: conhost.exe PID: 6284 Parent PID: 6236

General

Start time:	10:42:58
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6292 Parent PID: 5940

General

Start time:	10:42:58
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs \Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force
Imagebase:	0x910000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB0CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DB0CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_f3yslelb.mfk.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mufbm2g2.2lz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.+IqbRRN1.20201127104302.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_f3yslelb.mfk.ps1	success or wait	1	6C956A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mufbm2g2.2lz.psm1	success or wait	1	6C956A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_f3yslelb.mfk.ps1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mufbm2g2.2lz.psm1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.+IqbRRN1.20201127104302.txt	unknown	3	ef bb bf	...	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.+IqbRRN1.20201127104302.txt	unknown	767	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 37 31 30 34 33 33 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 39 32 32 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201127104335..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6C951B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6C951B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DAF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile

Analysis Process: conhost.exe PID: 6348 Parent PID: 6292

General

Start time:	10:42:58
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6356 Parent PID: 5940

General

Start time:	10:42:58
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe' -Force
Imagebase:	0x910000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DB0CF06	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	6DB0CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8B5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8B5B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_xk5gz5yj.lnm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_z5ws434f.y2b.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.e7cWhL8o.20201127104302.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C951E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_xk5gz5yj.lnm.ps1	success or wait	1	6C956A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_z5ws434f.y2b.psm1	success or wait	1	6C956A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_xk5gz5yj.lnm.ps1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_z5ws434f.y2b.psm1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.e7cWhL8o.20201127104302.txt	unknown	3	ef bb bf	...	success or wait	1	6C951B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.e7cWhL8o.20201127104302.txt	unknown	713	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 37 31 30 34 33 34 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 39 32 32 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201127104344..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6C951B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DAF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile

Analysis Process: conhost.exe PID: 6436 Parent PID: 6356

General

Start time:	10:42:59
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe PID: 6700 Parent PID: 5940

General

Start time:	10:43:05
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Imagebase:	0x7d0000
File size:	10985472 bytes
MD5 hash:	9817218C055DB1B75D64DF2AE2F40F53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.578444505.0000000003711000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.510166428.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe PID: 6816 Parent PID: 3472

General

Start time:	10:43:11
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe'
Imagebase:	0xb00000
File size:	10985472 bytes
MD5 hash:	9817218C055DB1B75D64DF2AE2F40F53
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe PID: 7112 Parent PID: 3472

General

Start time:	10:43:21
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe'
Imagebase:	0x560000
File size:	10985472 bytes
MD5 hash:	9817218C055DB1B75D64DF2AE2F40F53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe PID: 4864 Parent PID: 3472

General

Start time:	10:43:30
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe'
Imagebase:	0x4b0000
File size:	10985472 bytes
MD5 hash:	9817218C055DB1B75D64DF2AE2F40F53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe PID: 1308 Parent PID: 3472

General

Start time:	10:43:39
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe'
Imagebase:	0xdc0000
File size:	10985472 bytes
MD5 hash:	9817218C055DB1B75D64DF2AE2F40F53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe PID: 1460
Parent PID: 3472

General

Start time:	10:43:48
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe'
Imagebase:	0x1f0000
File size:	10985472 bytes
MD5 hash:	9817218C055DB1B75D64DF2AE2F40F53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, Virustotal, Browse • Detection: 14%, Metadefender, Browse • Detection: 29%, ReversingLabs
Reputation:	low

Disassembly

Code Analysis