ID: 680462
Sample Name:
SecuriteInfo.com.Suspicious.Win32.Save.a.5066.21910
Cookbook: default.jbs
Time: 16:34:08
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

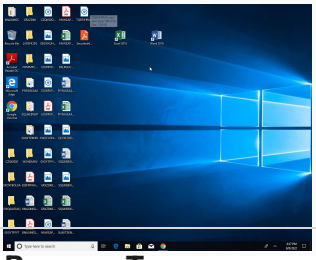
Windows Analysis Report

SecuriteInfo.com.Suspicious.Win32.Save.a.5066.21910

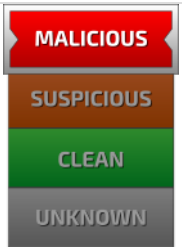
Overview

General Information

Sample Name:	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.21910 (renamed file extension from 21910 to exe)
Analysis ID:	680462
MD5:	836deaf4e5b11b..
SHA1:	4ef5dd4bde33a0..
SHA256:	a83b4422cdae17..
Tags:	exe
Infos:	



Detection



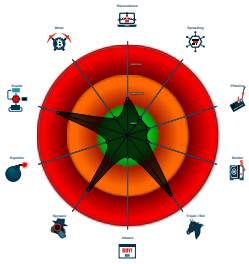
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- .NET source code references suspic…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe (PID: 6008 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe" MD5: 836DEAF4E5B11B7ED1A46FEA5850B33A)
  - cvtres.exe (PID: 6052 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "sylvainbaril@ocpi.com.my",
  "Password": "9v91sGq7r9M$",
  "Host": "mail.ocpi.com.my"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.245549949.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.245549949.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.245549949.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2f830:$a13: get_DnsResolver • 0x2e057:$a20: get_LastAccessed • 0x301c2:$a27: set_InternalServerPort • 0x304db:$a30: set_GuidMasterKey • 0x2e15e:$a33: get_Clipboard • 0x2e16c:$a34: get_Keyboard • 0x2f463:$a35: get_ShiftKeyDown • 0x2f474:$a36: get_AltKeyDown • 0x2e179:$a37: get_Password • 0x2ec13:$a38: get_PasswordHash • 0x2fc30:$a39: get_DefaultCredentials
00000001.00000000.244725171.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.244725171.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe.4f8d790.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe.4f8d790.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe.4f8d790.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x304f4:$s10: logins • 0x2ff5b:$s11: credential • 0x2c55e:$g1: get_Clipboard • 0x2c56c:$g2: get_Keyboard • 0x2c579:$g3: get_Password • 0x2d853:$g4: get_CtrlKeyDown • 0x2d863:$g5: get_ShiftKeyDown • 0x2d874:$g6: get_AltKeyDown
1.0.cvtres.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.0.cvtres.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 27 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Malware Analysis System Evasion

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

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

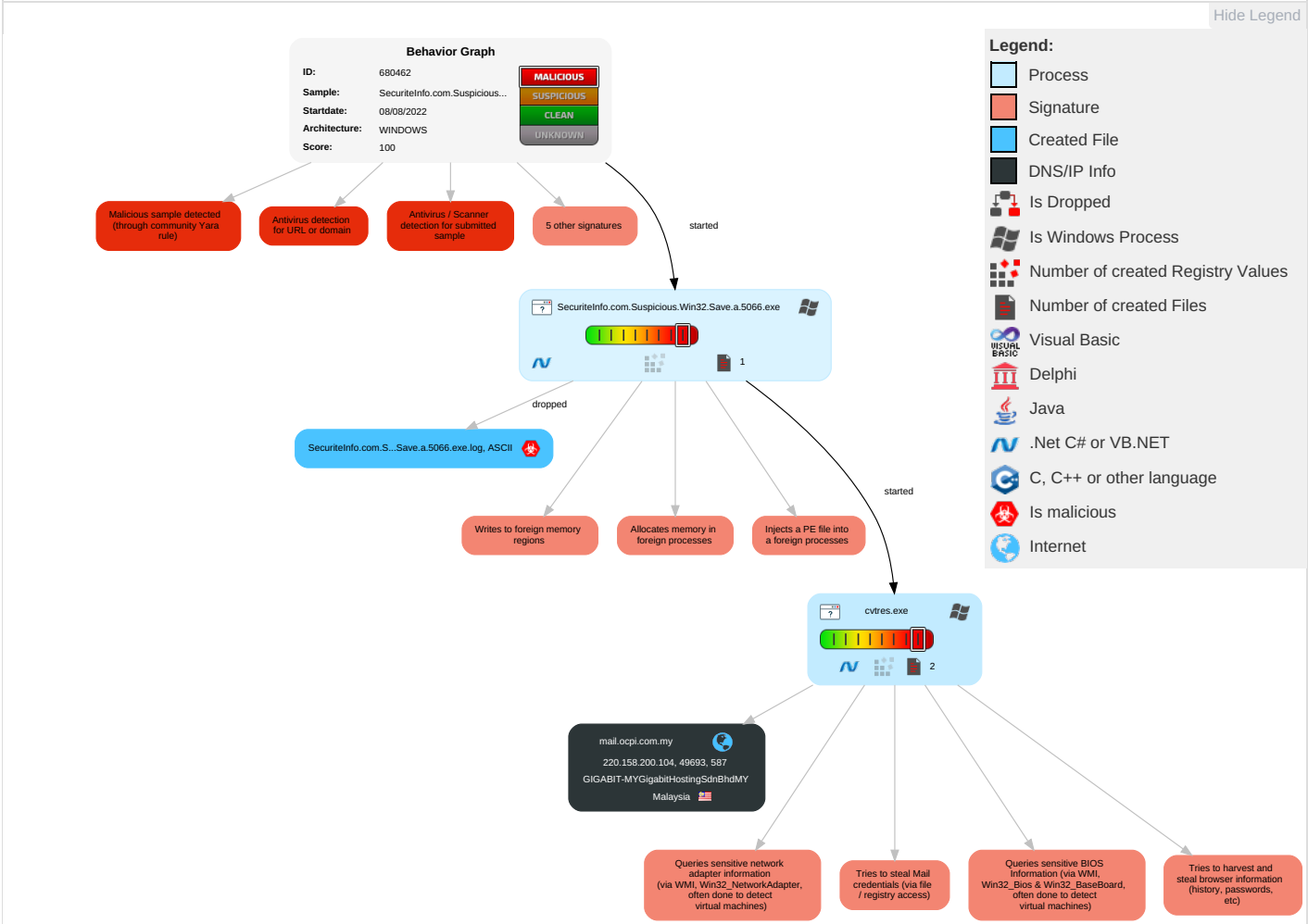
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

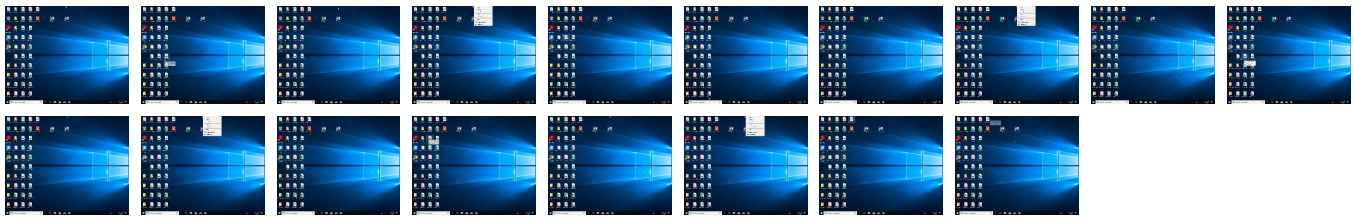
Behavior Graph



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.Suspicious.Win32.Save.a.5066.exe	25%	Virustotal		Browse
SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	100%	Avira	TR/Dropper.MSIL.Gen	
SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.cvtres.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.cvtres.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.cvtres.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.cvtres.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe.b40000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.cvtres.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.cvtres.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.ocpi.com.my	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://mail.ocpi.com.my	1%	Virustotal		Browse
http://mail.ocpi.com.my	100%	Avira URL Cloud	malware	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://DPVGsz.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.ocpi.com.my	220.158.200.104	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	cvtres.exe, 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://mail.ocpi.com.my	cvtres.exe, 00000001.00000002.512904675.0000000006C3F000.00000004.00000800.00020000.00000000.sdmp	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://cs-g2-crl.thawte.com/ThawteCSG2.crl0	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	false		high
http://crl.thawte.com/ThawtePCA.crl0	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	false		high
http://ocsp.thawte.com0	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	false	• URL Reputation: safe	unknown
http://DPVGsz.com	cvtres.exe, 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	cvtres.exe, 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	cvtres.exe, 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%%startupfolder%	cvtres.exe, 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://crl.thawte.com/ThawtePremiumServerCA.crl0	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	false		high
http://https://www.thawte.com/cps0	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	false		high
http://https://api.ipify.org%	cvtres.exe, 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.mozilla.com/0	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
220.158.200.104	mail.ocpi.com.my	Malaysia		55720	GIGABIT-MYGigabitHostingSdnBhdMY	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680462
Start date and time: 08/08/202216:34:08	2022-08-08 16:34:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.21910 (renamed file extension from 21910 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:	12
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@3/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:35:10	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe modified
16:35:13	API Interceptor	797x Sleep call for process: cvtres.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.3467126928258955
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2LDY3U21v:Q3La/KDLI4MWuPk21v
MD5:	DD8B7A943A5D834CEEAB90A6BBBF4781

SHA1:	2BED8D47DF1C0FF76B40811E5F11298BD2D06389
SHA-256:	E1D0A304B16BE51AE361E392A678D887AB0B76630B42A12D252EDC0484F0333B
SHA-512:	24167174EA259CAF57F65B9B9B9C113DD944FC957DB444C2F66BC656EC2E6565EFE4B4354660A5BE85CE4847434B3BDD4F7E05A9E9D61F4CC99FF0284DAA1C87
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.610837446996928
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe
File size:	252208
MD5:	836deaf4e5b11b7ed1a46fea5850b33a
SHA1:	4ef5dd4bde33a08e5c17da867ee4d14090673317
SHA256:	a83b4422cdae1748849530513cad3dae8e7ccee4f1117e696a4542156f1ae9e7
SHA512:	23bc084df7cf3e6ca758b2787f5cb08ed9f4b63c6e7025461e41840a441f9f61e429570fadafb6247571c42c59634f2e7c8226974a4ae9ede80adc5c82d76bec
SSDEEP:	6144:xi8lykGCl8Wymm0GcqwDhgBx2mtJwy7Aj:Nw5CPRGcqsgBx2cJwy7C
TLSH:	93349CF8765375CFC50BC8728AA84C64AA607CB7570BD103E45336DEAD5DA9B8F090A3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..X...D.....Nw... .....@.. .....`.....

File Icon

Icon Hash:	74ecc4d0f0e8ccc4

Static PE Info

General

Entrypoint:	0x43774e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F0CDFE [Mon Aug 8 08:49:02 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Thawte Code Signing CA - G2, O="Thawte, Inc.", C=US

Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/17/2012 5:00:00 PM 10/18/2013 4:59:59 PM
Subject Chain	• CN=Mozilla Corporation, OU=Release Engineering, O=Mozilla Corporation, L=Mountain View, S=California, C=US
Version:	3
Thumbprint MD5:	D686ED3797F476F0769F99DF2B0BCE73
Thumbprint SHA-1:	CAC47DBF634D24E9DC93072FE3C8EA6DC3946E89
Thumbprint SHA-256:	046B93E2298C5D45FB097329D2A7778302298B842664E3EBA261FF617D586F37
Serial:	3DA9386C2076F738EE246BB8E313A4D4

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x376f4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x418e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3bb98	0x1d98	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3e000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x376b0	0x1c	.text
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	0x35754	0x35800	False	0.8646548262266355	data	7.743635131824094	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x418e	0x4200	False	0.1376065340909091	data	3.022311948175261	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

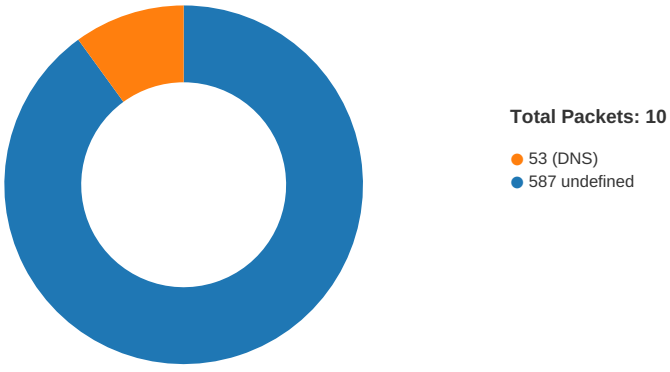
Name	RVA	Size	Type	Language	Country
RT_ICON	0x381a0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x38608	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x396b0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x3bc58	0x30	data		
RT_VERSION	0x3bc88	0x31c	data		
RT_MANIFEST	0x3bfa4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 16:35:19.212708950 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:19.480614901 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:19.480779886 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:20.197417021 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:20.197813034 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:20.465657949 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:20.477567911 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:20.745781898 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:20.746294022 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:21.053112984 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:23.238497972 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:23.292165995 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:23.400872946 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:23.668661118 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:23.668735027 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:23.669408083 CEST	587	49693	220.158.200.104	192.168.2.3
Aug 8, 2022 16:35:23.669513941 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:23.692826986 CEST	49693	587	192.168.2.3	220.158.200.104
Aug 8, 2022 16:35:23.960593939 CEST	587	49693	220.158.200.104	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 16:35:19.148879051 CEST	51578	53	192.168.2.3	8.8.8.8
Aug 8, 2022 16:35:19.171308994 CEST	53	51578	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 16:35:19.148879051 CEST	192.168.2.3	8.8.8.8	0x937b	Standard query (0)	mail.ocpi.com.my	A (IP address)	IN (0x0001)

DNS Answers

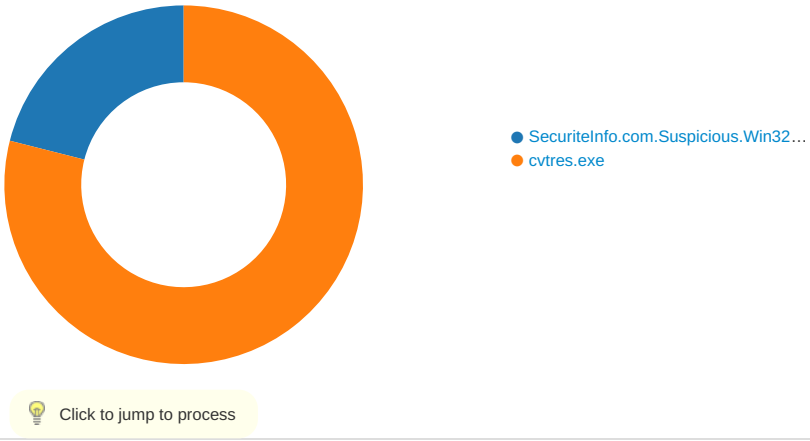
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 16:35:19.171308994 CEST	8.8.8.8	192.168.2.3	0x937b	No error (0)	mail.ocpi.com.my		220.158.200.104	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 16:35:20.197417021 CEST	587	49693	220.158.200.104	192.168.2.3	220-lion2.sfdns.net ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 22:35:20 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 16:35:20.197813034 CEST	49693	587	192.168.2.3	220.158.200.104	EHLO 358075
Aug 8, 2022 16:35:20.465657949 CEST	587	49693	220.158.200.104	192.168.2.3	250-lion2.sfdns.net Hello 358075 [102.129.143.3] 250-SIZE 104857600 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 16:35:20.477567911 CEST	49693	587	192.168.2.3	220.158.200.104	AUTH login c3lsdmFpbmJhcmlsQG9jcGkuY29tLm15
Aug 8, 2022 16:35:20.745781898 CEST	587	49693	220.158.200.104	192.168.2.3	334 UGFzc3dvcmQ6
Aug 8, 2022 16:35:23.238497972 CEST	587	49693	220.158.200.104	192.168.2.3	535 Incorrect authentication data
Aug 8, 2022 16:35:23.400872946 CEST	49693	587	192.168.2.3	220.158.200.104	MAIL FROM:<sylvainbaril@ocpi.com.my>
Aug 8, 2022 16:35:23.668735027 CEST	587	49693	220.158.200.104	192.168.2.3	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe PID: 6008, Parent PID: 5256

General

Target ID:	0
Start time:	16:35:09
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe"
Imagebase:	0xb40000
File size:	252208 bytes
MD5 hash:	836DEAF4E5B11B7ED1A46FEA5850B33A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.248323120.0000000004AAA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.248323120.0000000004AAA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.248323120.0000000004AAA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D14C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Suspicious.Win32.Save.a.5066.exe.log	0	226	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0	success or wait	1	6D14C907	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	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE1CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD703DE	ReadFile

Analysis Process: cvtres.exe PID: **6052**, Parent PID: **6008**

General

Target ID:	1
Start time:	16:35:10
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Imagebase:	0xa60000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
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: 00000001.00000000.245549949.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.245549949.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.245549949.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.244725171.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.244725171.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.244725171.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.245291051.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.245291051.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.245291051.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.509237498.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.509237498.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.509237498.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.244974805.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.244974805.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.244974805.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.511164792.0000000006921000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

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	6CE3CF06	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	6CE3CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	8173	end of file	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	4095	success or wait	1	6CE1CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	8173	end of file	1	6CE1CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC81B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	4096	success or wait	1	6BC81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	4096	end of file	1	6BC81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	8173	end of file	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	4096	success or wait	1	6BC81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.config	unknown	4096	end of file	1	6BC81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC81B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6BC81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC81B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BC81B4F	ReadFile

Disassembly

No disassembly