ID: 753413
Sample Name: SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe
Cookbook: default.jbs
Time: 19:29:07
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

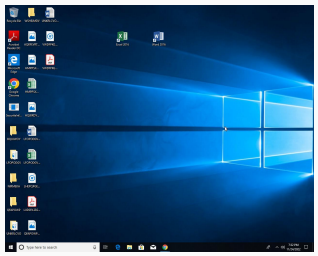
Windows Analysis Report

SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe

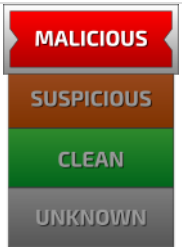
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe
Analysis ID:	753413
MD5:	2015410bb46bda.
SHA1:	f500da9df562378.
SHA256:	c36284bc37b2aa..
Tags:	AveMariaRAT exe
Infos:	



Detection



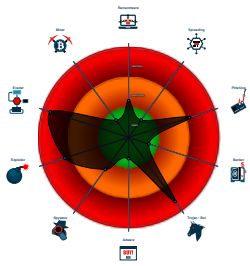
AveMaria, UACMe

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Increases the number of concurrent…
- Contains functionality to hide user a…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe (PID: 5264 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe MD5: 2015410BB46BDA0BD98BE49F2CA03E00)
  - powershell.exe (PID: 5208 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\hAwKqJPm.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5220 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hAwKqJPm" /XML "C:\Users\user\AppData\Local\Temp\tmp58FB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe (PID: 5584 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe MD5: 2015410BB46BDA0BD98BE49F2CA03E00)
- hAwKqJPm.exe (PID: 868 cmdline: C:\Users\user\AppData\Roaming\hAwKqJPm.exe MD5: 2015410BB46BDA0BD98BE49F2CA03E00)
  - schtasks.exe (PID: 3600 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hAwKqJPm" /XML "C:\Users\user\AppData\Local\Temp\tmp9691.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - hAwKqJPm.exe (PID: 1976 cmdline: C:\Users\user\AppData\Roaming\hAwKqJPm.exe MD5: 2015410BB46BDA0BD98BE49F2CA03E00)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "leekong.duckdns.org",
  "port": 6640
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x97f20:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x97f20:$c1: Elevation:Administrator!new:
00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AveMaria_31d2bce9	unknown	unknown	• 0x94678:$a1: cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q • 0x92edc:$a2: SMTP Password • 0x91aa8:$a3: select signon_realm, origin_url, username_value, password_value from logins • 0x97f20:$a4: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x94568:$a5: for /F "usebackq tokens=*" %%A in (" • 0x92768:$a6: \Torch\User Data\Default\Login Data • 0x98040:$a7: /n:%temp%\ellocnak.xml • 0x98070:$a9: Hey I'm Admin • 0x92cb4:$a10: \logins.json • 0x92dbc:$a10: \logins.json • 0x936a0:$a11: Accounts\Account.rec0 • 0x94330:$a13: Ave_Maria Stealer OpenSource github Link: https://github.com/syohex/java-simple-mine-sweeper

Click to see the 44 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.400000.0.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2c1f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
6.0.SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.400000.0.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2c1f0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x2c1f0:$c1: Elevation:Administrator!new:
6.0.SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.400000.0.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x266e0:$a1: \Opera Software\Opera Stable\Login Data • 0x269e0:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x261d8:$a3: \Google\Chrome\User Data\Default\Login Data
6.0.SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.400000.0.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
6.0.SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 212 entries

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ET TROJAN Warzone RAT Response (Inbound) - Source IP: 103.150.8.47 - Destination IP: 192.168.2.3

Timestamp:	103.150.8.47192.168.2.36640496912038897 11/24/22-19:30:17.744742
SID:	2038897
Source Port:	6640
Destination Port:	49691
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT PingResponse - Source IP: 192.168.2.3 - Destination IP: 103.150.8.47	
Timestamp:	192.168.2.3103.150.8.474969166402851946 11/24/22-19:31:57.790282
SID:	2851946
Source Port:	49691
Destination Port:	6640
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT PingCommand - Source IP: 103.150.8.47 - Destination IP: 192.168.2.3	
Timestamp:	103.150.8.47192.168.2.36640496912851945 11/24/22-19:31:57.787821
SID:	2851945
Source Port:	6640
Destination Port:	49691
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT ListPasswordsCommand - Source IP: 103.150.8.47 - Destination IP: 192.168.2.3	
Timestamp:	103.150.8.47192.168.2.36640496912851933 11/24/22-19:30:18.197244
SID:	2851933
Source Port:	6640
Destination Port:	49691
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT BeaconResponse - Source IP: 192.168.2.3 - Destination IP: 103.150.8.47	
Timestamp:	192.168.2.3103.150.8.474969166402852357 11/24/22-19:30:17.889863
SID:	2852357
Source Port:	49691
Destination Port:	6640
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT InitializePacket - Source IP: 103.150.8.47 - Destination IP: 192.168.2.3	
Timestamp:	103.150.8.47192.168.2.36640496912852356 11/24/22-19:31:37.787359
SID:	2852356
Source Port:	6640
Destination Port:	49691
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound) - Source IP: 103.150.8.47 - Destination IP: 192.168.2.3	
Timestamp:	103.150.8.47192.168.2.36640496912851895 11/24/22-19:30:17.744742
SID:	2851895
Source Port:	6640
Destination Port:	49691
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Yara detected UACMe UAC Bypass tool

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected AveMaria stealer

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information

Yara detected AveMaria stealer

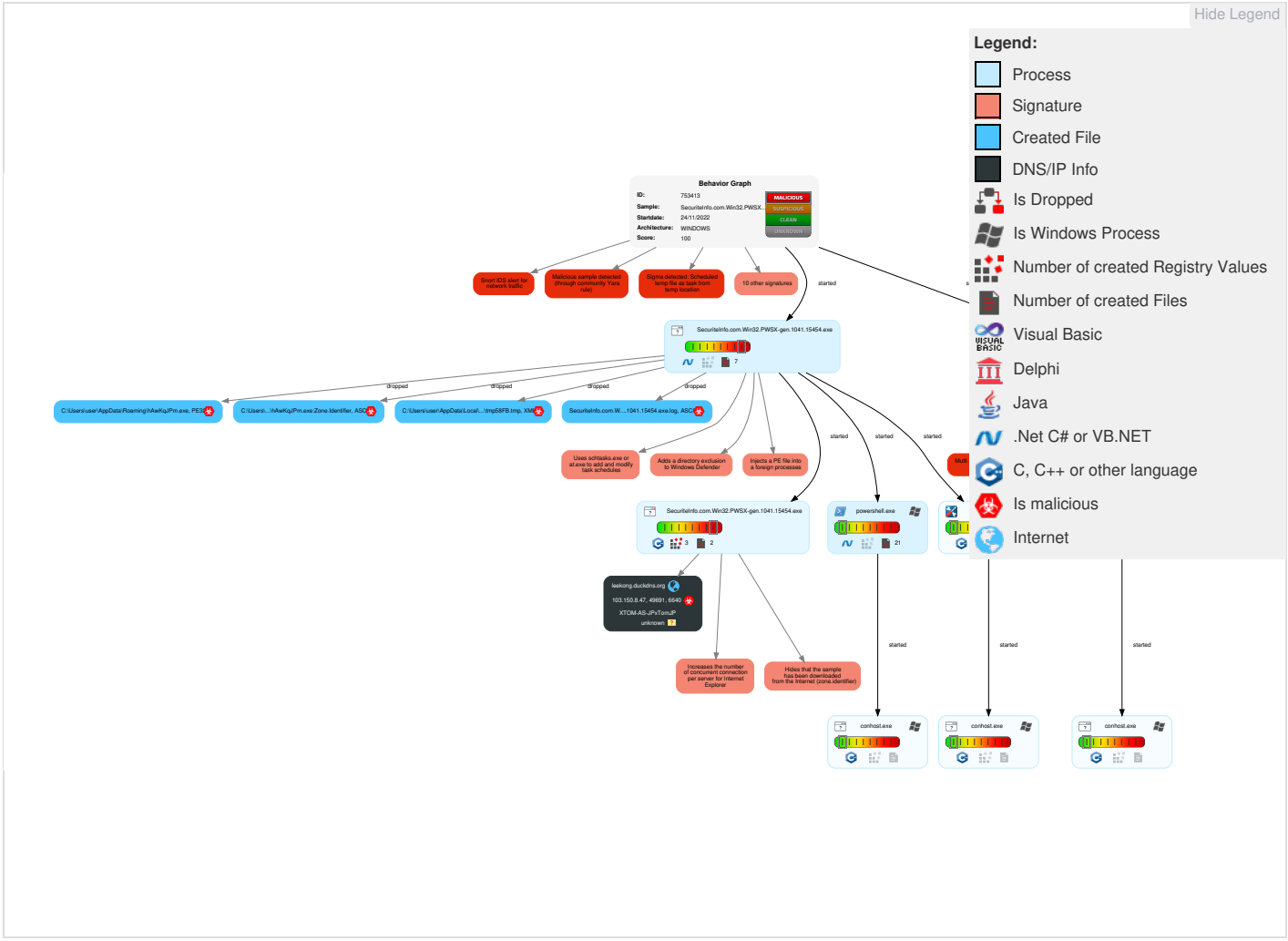
Remote Access Functionality

Yara detected AveMaria stealer

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	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	3 Masqueradi ng	1 1 Input Capture	2 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	1 Endpoint Denial of Service
Default Accounts	Scheduled Task/Job	Boot or Logon Initializatio n Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualizatio n/Sandbox Evasion	Security Account Manager	2 1 Virtualizatio n/Sandbox Evasion	SMB/Wind ows Admin Shares	Data from Network Shared Drive	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)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.commo n	Rc.commo n	1 Hidden Users	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic ation	Jamming or Denial of Service		Abuse Accessibilit y Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Manageme nt	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromis e	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

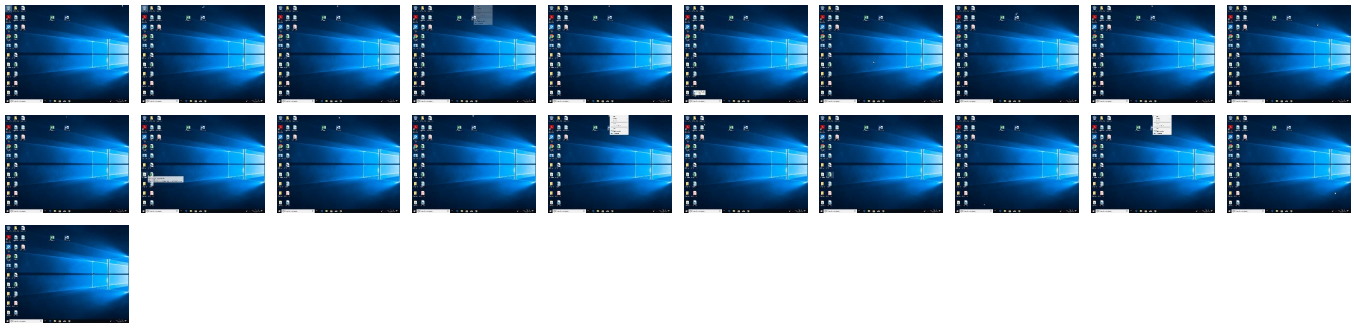
Behavior Graph



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.1041.15454.exe	20%	ReversingLabs		
SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\hAwKqJPm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\hAwKqJPm.exe	20%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
6.3.SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.de8600.2.unpack	100%	Avira	TR/Downloader.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnX	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-d	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnG	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.typography.netD	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.fontbureau.comonyd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s_tr	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://en.wikipedia	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comionm	0%	URL Reputation	safe	
http://www.fontbureau.comn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comx	0%	URL Reputation	safe	
leekong.duckdns.org	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF2	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceco	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlicr	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comG	0%	Avira URL Cloud	safe	
http://www.fontbureau.comK	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiced	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomF2	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritog	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnion	0%	Avira URL Cloud	safe	
http://www.sakkal.com-s	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ww.mK	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comegQ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
leekong.duckdns.org	103.150.8.47	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
leekong.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnX	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246180301.000000000621700.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a-d	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247494081.000000000621B00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comceco	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254614525.000000000621700.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.288947142.000000000621B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254219136.000000000621700.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254731944.000000000621C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254219136.000000000621700.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersiva	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254219136.000000000621700.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnG	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246180301.000000000621700.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246129356.000000000621800.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comG	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245634926.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247567253.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244950903.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245165040.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244885604.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247480222.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244827108.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244764143.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245711171.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245899283.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245260378.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246660475.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245075024.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246297100.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247170656.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245317017.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247119623.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245431681.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246576079.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244800921.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246100788.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245634926.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247567253.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244950903.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245165040.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244885604.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244712367.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247480222.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244827108.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244764143.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245711171.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244742234.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245899283.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245260378.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246660475.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.0000000007422000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245075024.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246297100.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247170656.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245317017.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247119623.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245431681.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/9	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247494081.000000000621B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248068026.000000000621D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248125653.000000000621D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.00000000074220 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.00000000074220 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF2	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250306044.000000000621C0 00.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/2	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247494081.000000000621B0 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comonyd	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250362269.000000000621E0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250076896.000000000 621D000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.PWSX-ge n.1041.15454.exe, 00000000.00000003.2503 06044.000000000621C000.00000004.00000800 .00020000.00000000.sdmp, SecuriteInfo.co m.Win32.PWSX-gen.1041.15454.exe, 0000000 0.00000003.251108759.000000000621C000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.251222842.000000000621C0 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248068026.000000000621D0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248125653.000000000 621D000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/syohex/java-simple-mine-sweeper-instInitWindows	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.287016185.00000000048F80 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.285102009.000000000 45D0000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.PWSX-ge n.1041.15454.exe, 00000000.00000002.2797 18323.000000000354E000.00000004.00000800 .00020000.00000000.sdmp, hAwKqJPm.exe, 0 0000005.00000002.303636466.0000000002AFE 000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000006.00000003.278810963.000000000 00DF0000.00000004.00000020.00020000.0000 0000.sdmp, SecuriteInfo.com.Win32.PWSX-g en.1041.15454.exe, 00000006.00000000.268 659603.0000000000426000.00000040.0000040 0.00020000.00000000.sdmp, SecuriteInfo.c om.Win32.PWSX-gen.1041.15454.exe, 000000 06.00000003.278763102.0000000000DE4000.0 0000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 0 0000006.00000003.279232900.0000000000DF8 000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000006.00000003.279160265.000000000 00DFC000.00000004.00000020.00020000.0000 0000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.00000000074220 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248068026.000000000621D0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248125653.000000000 621D000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/s_tr	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247494081.000000000621B0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248068026.000000000 621D000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.PWSX-ge n.1041.15454.exe, 00000000.00000003.2481 25653.000000000621D000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

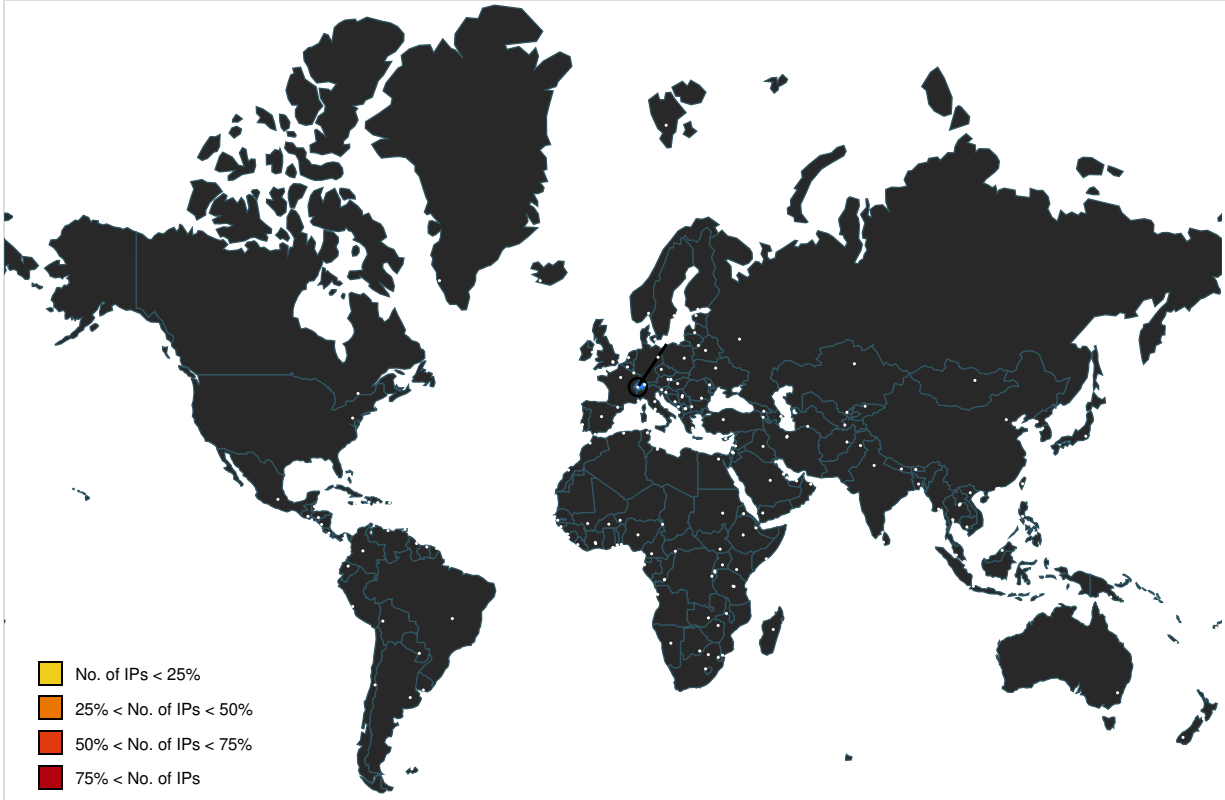
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlicr	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250362269.000000000621E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250306044.000000000621C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.279718323.000000000354E000.00000004.00000800.00020000.00000000.sdmp, hAwKqJPm.exe, 00000005.00000002.303636466.0000000002AFE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comiced	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250362269.000000000621E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250306044.000000000621C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000007422000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246736589.000000006217000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246673230.0000000006217000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250076896.000000000621D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comK	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250362269.000000000621E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250076896.000000000621D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250306044.000000000621C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250009805.000000000621C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomF2	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250362269.000000000621E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgritog	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250076896.000000000621D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250009805.000000000621C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.wikipedia	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244541126.00000000062330 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244510338.000000000 6233000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.PWSX-ge n.1041.15454.exe, 00000000.00000003.2444 85601.0000000006232000.00000004.00000800 .00020000.00000000.sdmp, SecuriteInfo.co m.Win32.PWSX-gen.1041.15454.exe, 0000000 0.00000003.244567187.0000000006233000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244597426.00000000062330 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248068026.000000000621D0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248125653.000000000 621D000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254614525.00000000062170 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.288947142.000000000 621B000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.PWSX-ge n.1041.15454.exe, 00000000.00000003.2542 19136.0000000006217000.00000004.00000800 .00020000.00000000.sdmp, SecuriteInfo.co m.Win32.PWSX-gen.1041.15454.exe, 0000000 0.00000003.254731944.000000000621C000.00 000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250076896.000000000621D0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250009805.000000000 621C000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244875435.00000000062160 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.00000000074220 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.00000000074220 00.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnion	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246006407.00000000062170 00.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com-s	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248060428.00000000062450 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248114380.000000000 6244000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.PWSX-ge n.1041.15454.exe, 00000000.00000003.2480 94904.0000000006246000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246129356.00000000062180 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000 7422000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.PWSX-ge n.1041.15454.exe, 00000000.00000003.2460 06407.0000000006217000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.00000000074220 00.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/ww.mK	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248068026.000000000621D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248125653.000000000621D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comegQ	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245634926.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247567253.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244950903.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245165040.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244885604.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247480222.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244827108.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244764143.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245711171.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245899283.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245260378.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246660475.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245075024.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246297100.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247170656.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245317017.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247119623.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.245431681.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246576079.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.244800921.000000000622B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.246100788.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250076896.000000000621D000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comionm	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254614525.000000006217000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.288947142.000000006 21B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.254731944.000000000621C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comn	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250362269.000000000621E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.251108759.000000000 621C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.247494081.000000000621B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000 7422000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248068026.000000000621D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.248125653.000000000621D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000002.289129685.000000000742200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comx	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250362269.000000000621E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe, 00000000.00000003.250306044.000000000 621C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.150.8.47	leekong.duckdns.org	unknown	?	4785	XTOM-AS-JPxTomJP	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753413
Start date and time:	2022-11-24 19:29:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.PWSX-gen.1041.15454.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:	22
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.phis.troj.expl.evad.winEXE@15/9@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsp.digicert.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior 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
19:30:05	API Interceptor	2x Sleep call for process: SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe modified
19:30:09	API Interceptor	33x Sleep call for process: powershell.exe modified
19:30:10	Task Scheduler	Run new task: hAwKqJPm path: C:\Users\user\AppData\Roaming\hAwKqJPm.exe
19:30:21	API Interceptor	2x Sleep call for process: hAwKqJPm.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.Win32.PWSX-gen.1041.15454.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.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\hAwKqJPm.exe.log

Process:	C:\Users\user\AppData\Roaming\hAwKqJPm.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
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\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22016
Entropy (8bit):	5.598831434263491
Encrypted:	false
SSDEEP:	384:2tCR3kGlTe9ly6uP4HyNB73USBxnejibiJ9g5SJ3uyC1+m021AVrdACsf0A+izYb:zVyy/PtBzU4xeuP5cuCXFb
MD5:	4948D58E4C9B37FFC0BFA376FB43E44A
SHA1:	9359741CDD6E3D4F6BA91CAD50DBEAFDFE4257E0
SHA-256:	5938DFEEB96742412A15B0D54333F7EAD01178A31ED4E1197414E3F98FF1C262
SHA-512:	0A41A2FB6953F8BB43012E40C76D9D45DD8468D3608C032D782AD273798BC5BEB28F3B38E0B33119D432CBF34B518488ABA335A3D47FC2F033B2925B3AA2854
Malicious:	false
Preview:	@...e.....7.....7.....@.....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_rs2uu4tt.g22.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zg3r1ixe.pyh.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp58FB.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe

File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.154045872002826
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt4axvn:cge4MYrFdOFzOzN33ODOiDdKrsuT3v
MD5:	2829DB7F9375335D00676E8A8D3325E1
SHA1:	1213283AA2FD79C2FDEA070BFE36A442FF0B0328
SHA-256:	7B9F5D4256077489D2AB74BE27352F8AEC19BCD40AA1B630FEEBD023F60BF1AA
SHA-512:	74A317A95B1C82F6FA6170F5D48CA1CF757D710962CC32E643C76730F6105445DB406B939AFBD00F00325F7FBA80C034947F2FDABEF6F5CE4961FD6E92EE15D D
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\tmp9691.tmp

Process:	C:\Users\user\AppData\Roaming\hAwKqJPm.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.154045872002826
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt4axvn:cge4MYrFdOFzOzN33ODOiDdKrsuT3v
MD5:	2829DB7F9375335D00676E8A8D3325E1
SHA1:	1213283AA2FD79C2FDEA070BFE36A442FF0B0328
SHA-256:	7B9F5D4256077489D2AB74BE27352F8AEC19BCD40AA1B630FEEBD023F60BF1AA
SHA-512:	74A317A95B1C82F6FA6170F5D48CA1CF757D710962CC32E643C76730F6105445DB406B939AFBD00F00325F7FBA80C034947F2FDABEF6F5CE4961FD6E92EE15D D
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\hAwKqJPm.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	872960
Entropy (8bit):	7.69627043654526
Encrypted:	false
SSDEEP:	12288:XHmZJbxpDFv6d2tZKGxF9rOTE/oMwtXBE3QVmfVUQa8PbT6OZO2bUq0fjVZ5jSC:XHvd2tceX/nyR3VmfVDHbTLZOKYjkC
MD5:	2015410BB46BDA0BD98BE49F2CA03E00
SHA1:	F500DA9DF562378CD0565485489321D59FA1699C
SHA-256:	C36284BC37B2AAF39D2E911EF97AAC1FA583CA30D90F2CD006635F8F5BF0D7E1
SHA-512:	003A87FA2A9E6CBC2E12EDE2CBF78ABBE11EEC1635E0695406C421C496783DEFD9EC6659A1524D8481DBEED61155BB5EEBBE997EA0863E8590BBC69B3C8C C7E6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0..J.....i... .....@.. ....@.....h..O.....p..... ....H.....text....I... ...J..... ..`.rsrc...p.....L.....@..@.rel oc.....P.....@..B.....h.....H.....j..TE.....V.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3. *....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*^..}.....(.....(.....*....0..#.....{.....,...{.....~....o.....*&..(.....*....0..#.....{.....,...{.....~....o .....*..0..+.....,..{.....+....,...{....o.....(...

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.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):	7.69627043654526
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.1041.15454.exe
File size:	872960
MD5:	2015410bb46bda0bd98be49f2ca03e00
SHA1:	f500da9df562378cd0565485489321d59fa1699c
SHA256:	c36284bc37b2aaf39d2e911ef97aac1fa583ca30d90f2cd006635f8f5bf0d7e1
SHA512:	003a87fa2a9e6cbc2e12ede2cbf78abbe11eec1635e0695406c421c496783defd9ec6659a1524d8481dbeed61155bb5eebbe997ea0863e8590bbc69b3c8cc7e6
SSDEEP:	12288:XHmZJbxpDFv6d2tZKGxF9rOTE/oMwtXBE3QVmfVUQa8PbT6OZO2bUq0fjVZ5jSC:XHvd2tceX/nyR3VmfVDHbTLZOKYjkC
TLSH:	07058DDF59613E08C29CBAB06817348C7EA194504948E1E4E7E917D95A3BFBDCB8123F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0..J.....i... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d690e
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:	0x637F84B3 [Thu Nov 24 14:50:27 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]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd68bc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x370	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0xd4914	0xd4a00	False	0.8398414535567313	SysEx File -	7.699539405299492	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x370	0x400	False	0.365234375	data	2.789007112227322	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	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_VERSION	0xd8058	0x314	data		

Imports

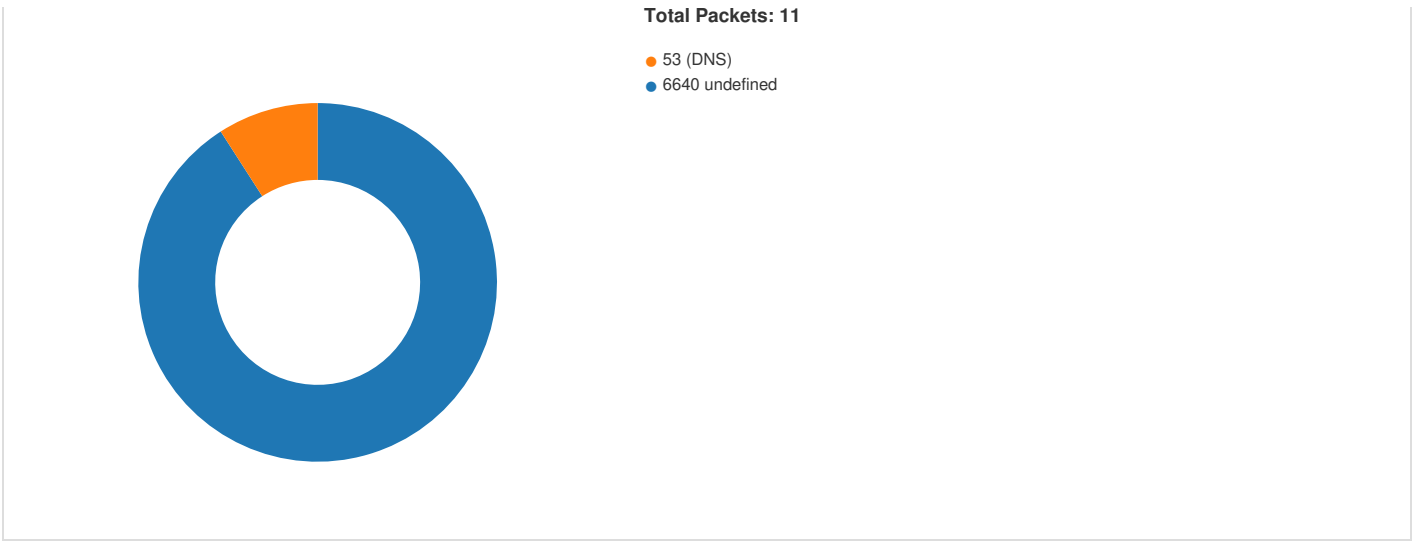
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
103.150.8.47192.168.2.36640496912038897 11/24/22-19:30:17.744742	TCP	2038897	ET TROJAN Warzone RAT Response (Inbound)	6640	49691	103.150.8.47	192.168.2.3
192.168.2.3103.150.8.474969166402851946 11/24/22-19:31:57.790282	TCP	2851946	ETPRO TROJAN Ave Maria/Warzone RAT PingResponse	49691	6640	192.168.2.3	103.150.8.47
103.150.8.47192.168.2.36640496912851945 11/24/22-19:31:57.787821	TCP	2851945	ETPRO TROJAN Ave Maria/Warzone RAT PingCommand	6640	49691	103.150.8.47	192.168.2.3
103.150.8.47192.168.2.36640496912851933 11/24/22-19:30:18.197244	TCP	2851933	ETPRO TROJAN Ave Maria/Warzone RAT ListPasswordsCommand	6640	49691	103.150.8.47	192.168.2.3
192.168.2.3103.150.8.474969166402852357 11/24/22-19:30:17.889863	TCP	2852357	ETPRO TROJAN Ave Maria/Warzone RAT BeaconResponse	49691	6640	192.168.2.3	103.150.8.47
103.150.8.47192.168.2.36640496912852356 11/24/22-19:31:37.787359	TCP	2852356	ETPRO TROJAN Ave Maria/Warzone RAT InitializePacket	6640	49691	103.150.8.47	192.168.2.3
103.150.8.47192.168.2.36640496912851895 11/24/22-19:30:17.744742	TCP	2851895	ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)	6640	49691	103.150.8.47	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:30:17.173063040 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:30:17.459017992 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:30:17.459163904 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:30:17.744741917 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:30:17.804780960 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:30:17.889863014 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:30:18.197243929 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:30:18.215589046 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:30:18.543471098 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:30:37.756028891 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:30:37.757914066 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:30:38.082035065 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:30:57.758604050 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:30:57.759512901 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:30:58.084768057 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:31:17.771068096 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:31:17.772058964 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:31:18.099214077 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:31:37.787358999 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:31:37.789005995 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:31:38.112308979 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:31:57.787821054 CET	6640	49691	103.150.8.47	192.168.2.3
Nov 24, 2022 19:31:57.790282011 CET	49691	6640	192.168.2.3	103.150.8.47
Nov 24, 2022 19:31:58.113883018 CET	6640	49691	103.150.8.47	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:30:17.056688070 CET	54397	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:30:17.168728113 CET	53	54397	8.8.8.8	192.168.2.3

DNS Queries

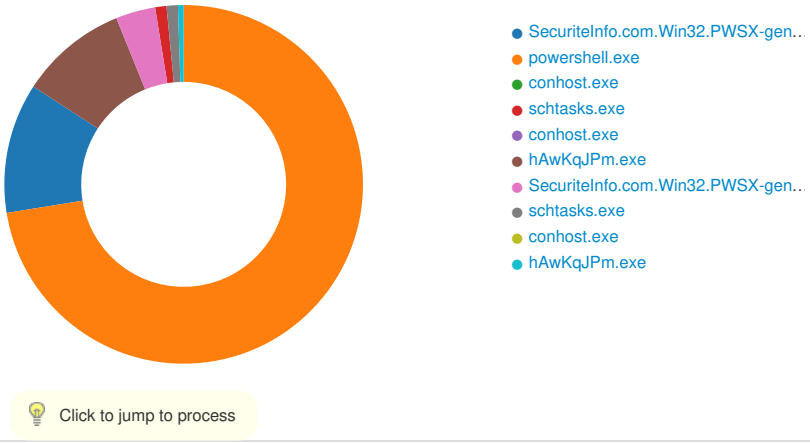
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:30:17.056688070 CET	192.168.2.3	8.8.8.8	0x7da1	Standard query (0)	leekong.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 19:30:17.168728113 CET	8.8.8.8	192.168.2.3	0x7da1	No error (0)	leekong.duckdns.org		103.150.8.47	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe PID: **5264**, Parent PID: **3452**

General

Target ID:	0
Start time:	19:29:58
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe
Imagebase:	0xed0000
File size:	872960 bytes
MD5 hash:	2015410BB46BDA0BD98BE49F2CA03E00
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000000.00000002.287016185.00000000048F8000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.279718323.000000000354E000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.279718323.000000000354E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.279718323.000000000354E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.279718323.000000000354E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.279718323.000000000354E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000000.00000002.279718323.000000000354E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.285102009.00000000045D0000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.285102009.00000000045D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.285102009.00000000045D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.285102009.00000000045D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000000.00000002.285102009.00000000045D0000.00000004.00000800.00020000.00000000.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	6D1BCF06	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	6D1BCF06	unknown
C:\Users\user\AppData\Roaming\hAwKqJPm.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	6C00DD66	CopyFileW
C:\Users\user\AppData\Roaming\hAwKqJPm.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C00DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp58FB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C007038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp58FB.tmp	success or wait	1	6C006A95	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\Roaming\hAwKqJPm.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 fd 7f 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 4a 0d 00 00 06 00 00 00 00 00 00 0e 69 0d 00 00 20 00 00 00 fd 0d 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 0d 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.$PELc0Ji @ @	success or wait	4	6C00DD66	CopyFileW
C:\Users\user\AppData\Roaming\hAwKqJPm.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	6C00DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp58FB.tmp	0	1595	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 68 61 72 64 7a 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	6C001B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.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	6D4CC907	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	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: powershell.exe PID: **5208**, Parent PID: **5264**

General

Target ID:	1
Start time:	19:30:07
Start date:	24/11/2022
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\hAwKqJPm.exe
Imagebase:	0xc10000
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__PSscriptPolicyTest_zg3r1ixe.pyh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C001E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rs2uu4tt.g22.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C001E60	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	6D1BCF06	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	6D1BCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zg3r1ixe.pyh.ps1	success or wait	1	6C006A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rs2uu4tt.g22.psm1	success or wait	1	6C006A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zg3r1ixe.pyh.ps1	0	1	31	1	success or wait	1	6C001B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rs2uu4tt.g22.psm1	0	1	31	1	success or wait	1	6C001B4F	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 37 14 00 00 1a 00 00 00 fd 0e fd 05 fd 08 fd 08 fd 08 00 00 37 01 fd 00 0a 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e77@	success or wait	1	6D4876FC	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	6D4876FC	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	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6D4876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 68 38 40 01 67 38 40 01 10 6f 40 01 11 6f 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 05 0e fd 00 06 0e fd 00 04 0e fd 00 07 0e fd 00 08 0e fd 00 12 6f 40 01 2a 29 40 01 1f 29 40 01 4d 64 40 01 5d 64 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@h8@g8@o@o@D@D@@M@<M@$M@8M@?M@o@*)@)@Md@]d@	success or wait	11	6D4876FC	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	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D19CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D1A1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	6D1A203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	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	6C001B4F	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	6C001B4F	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	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: conhost.exe PID: **5176**, Parent PID: **5208**

General

Target ID:	2

Start time:	19:30:07
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **5220**, Parent PID: **5264**

General

Target ID:	3
Start time:	19:30:07
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hAwKqJPm" /XML "C:\Users\user\AppData\Local\Temp\tmp58FB.tmp
Imagebase:	0xe50000
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\tmp58FB.tmp	unknown	2	success or wait	1	E5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp58FB.tmp	unknown	1596	success or wait	1	E5ABD9	ReadFile

Analysis Process: conhost.exe PID: **1832**, Parent PID: **5220**

General

Target ID:	4
Start time:	19:30:07
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: hAwKqJPm.exe PID: **868**, Parent PID: **1080**

General

Target ID:	5
Start time:	19:30:10
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Roaming\hAwKqJPm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hAwKqJPm.exe
Imagebase:	0x510000
File size:	872960 bytes
MD5 hash:	2015410BB46BDA0BD98BE49F2CA03E00
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000005.00000002.303636466.0000000002AFE000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000005.00000002.303636466.0000000002AFE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000005.00000002.303636466.0000000002AFE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.303636466.0000000002AFE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000005.00000002.303636466.0000000002AFE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000005.00000002.303636466.0000000002AFE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, 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	6D1BCF06	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	6D1BCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp9691.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C007038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hAwKqJPm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9691.tmp	success or wait	1	6C006A95	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\tmp9691.tmp	0	1595	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 68 61 72 64 7a 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	6C001B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hAwKqJPm.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	6D4CC907	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	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	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	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe PID: **5584**, Parent PID: **5264**

General

Target ID:	6
Start time:	19:30:11
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe
Imagebase:	0x680000
File size:	872960 bytes
MD5 hash:	2015410BB46BDA0BD98BE49F2CA03E00
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000003.278810963.0000000000DF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000006.00000003.278810963.0000000000DF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000006.00000003.278810963.0000000000DF0000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000000.268659603.0000000000426000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000006.00000000.268659603.0000000000426000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000006.00000000.268659603.0000000000426000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000003.278763102.0000000000DE4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000006.00000003.278763102.0000000000DE4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000006.00000003.278763102.0000000000DE4000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000006.00000000.268913110.0000000000562000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000006.00000000.268913110.0000000000562000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000006.00000003.279119713.0000000000DE4000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000006.00000003.279119713.0000000000DE4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000003.279160265.0000000000DFC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000006.00000003.279160265.0000000000DFC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000006.00000003.279160265.0000000000DFC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4242D1	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe:Zone.Identifier	success or wait	1	42100B	DeleteFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe	unknown	872960	success or wait	1	42218C	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.1041.15454.exe	unknown	872960	success or wait	1	42218C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WBR2T3PLXR	success or wait	1	4207B7	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPer1_0Server	dword	10	success or wait	1	424226	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	42423E	RegSetValueExA

Analysis Process: schtasks.exe PID: **3600**, Parent PID: **868**

General

Target ID:	17
Start time:	19:30:24
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hAwKqJPm" /XML "C:\Users\user\AppData\Local\Temp\tmp9691.tmp
Imagebase:	0xe50000
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\tmp9691.tmp	unknown	2	success or wait	1	E5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9691.tmp	unknown	1596	success or wait	1	E5ABD9	ReadFile

Analysis Process: conhost.exe PID: **2292**, Parent PID: **3600**

General

Target ID:	18
Start time:	19:30:24
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000

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: hAwKqJPm.exe PID: **1976**, Parent PID: **868**

General

Target ID:	19
Start time:	19:30:25
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Roaming\hAwKqJPm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hAwKqJPm.exe
Imagebase:	0x940000
File size:	872960 bytes
MD5 hash:	2015410BB46BDA0BD98BE49F2CA03E00
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

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\Roaming\hAwKqJPm.exe	unknown	872960	success or wait	1	42218C	ReadFile

Disassembly

No disassembly