ID: 356595
Sample Name:
SecuriteInfo.com.Win32.32289.26241
Cookbook: default.jbs
Time: 11:52:56
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

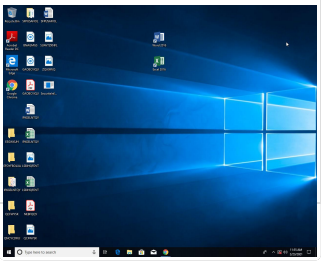
Analysis Report SecuriteInfo.com.Win32.32289.26241

Overview

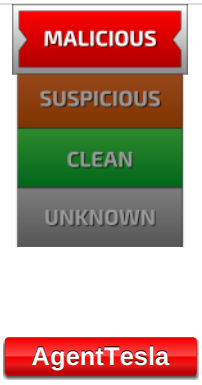
General Information

Sample Name:	SecuriteInfo.com.Win32.32289.26241 (renamed file extension from 26241 to exe)
Analysis ID:	356595
MD5:	c59f71a02c13a01..
SHA1:	59c60b6a90cec4...
SHA256:	983c3585908989..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

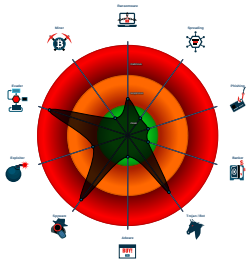


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Contains functionality to register a lo…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Win32.32289.exe (PID: 6228 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe' MD5: C59F71A02C13A01D95BF37C095895748)
  - schtasks.exe (PID: 6444 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\avJawOiuQtyAB' /XML 'C:\Users\user\AppData\Local\Temp\tmp7060.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Win32.32289.exe (PID: 6496 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe MD5: C59F71A02C13A01D95BF37C095895748)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "IplK5j4pUxwp",
  "URL: ": "https://WNhKF6NrBBD3PYwnVMvS.net",
  "To: ": "jason.samtani@rxcleco.com",
  "ByHost: ": "mail.privateemail.com:587",
  "Password: ": "A7HCE",
  "From: ": "jason.samtani@rxcleco.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.495792396.000000000311 2000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.495604124.00000000030D 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.495604124.00000000030D 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.251883452.000000000411 6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.491127410.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

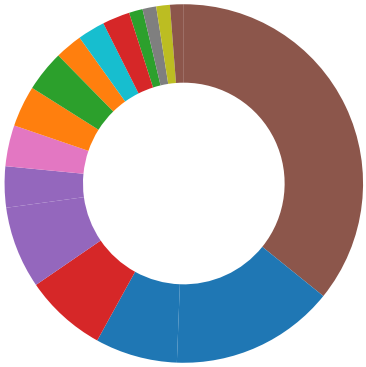
Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Win32.32289.exe.41672b0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.SecuriteInfo.com.Win32.32289.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Win32.32289.exe.2ed6bcc.1.raw .unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.SecuriteInfo.com.Win32.32289.exe.41672b0.4.raw .unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

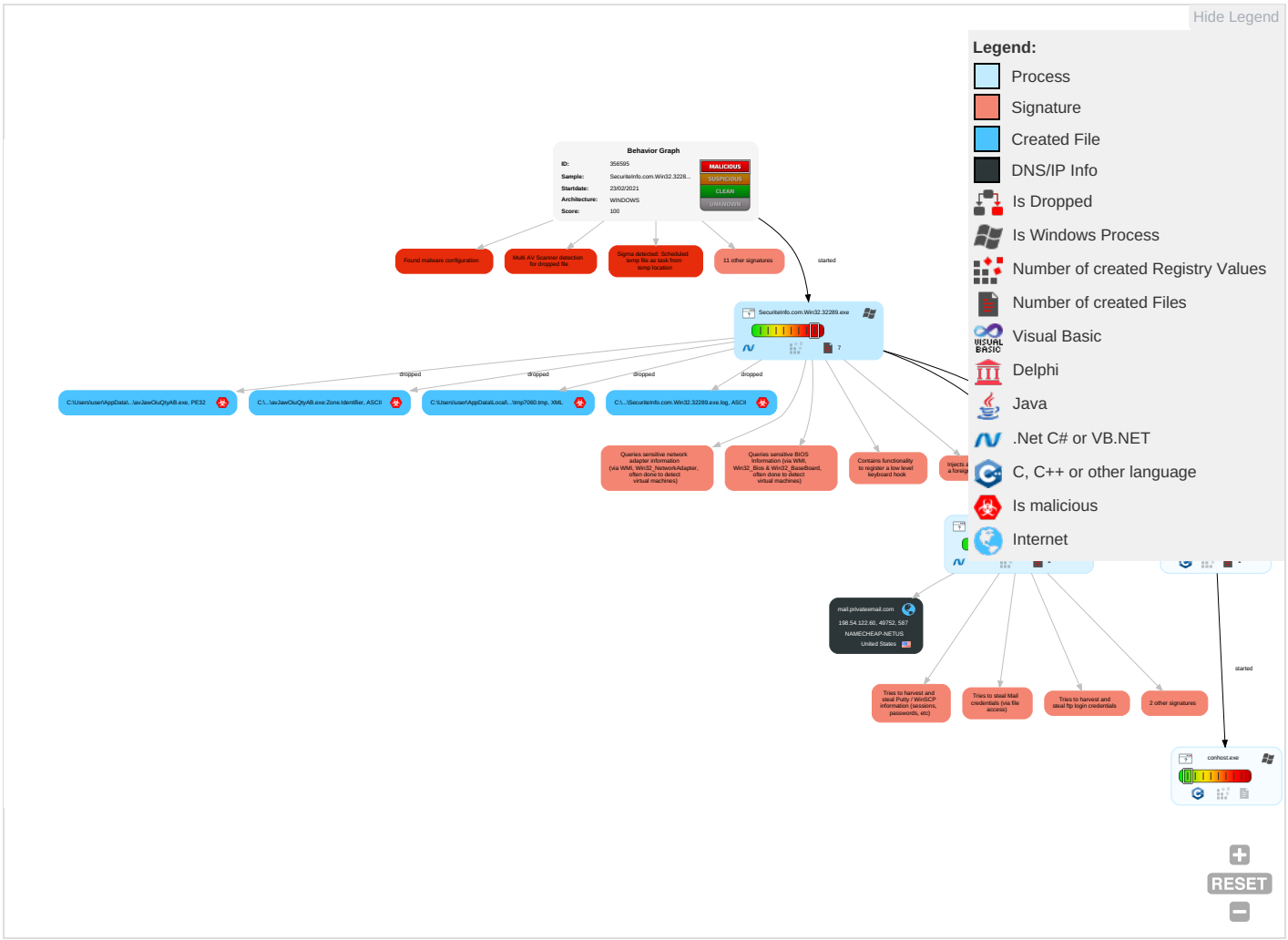
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stanc Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Appli Layer Prot
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Applicatio Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Protocol

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.32289.exe	28%	Virustotal		Browse
SecuriteInfo.com.Win32.32289.exe	35%	ReversingLabs	Win32.Trojan.Wacatac	
SecuriteInfo.com.Win32.32289.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\avJawOiuQtyAB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\avJawOiuQtyAB.exe	35%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.SecuriteInfo.com.Win32.32289.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
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/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comuec	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	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://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://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-u	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/l	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.comml	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r-e	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.carterandcone.com_	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.fontbureau.comd~	0%	Avira URL Cloud	safe	
http://www.fontbureau.comic	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/R	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://WNhKF6NrBBD3PYwnVMvS.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

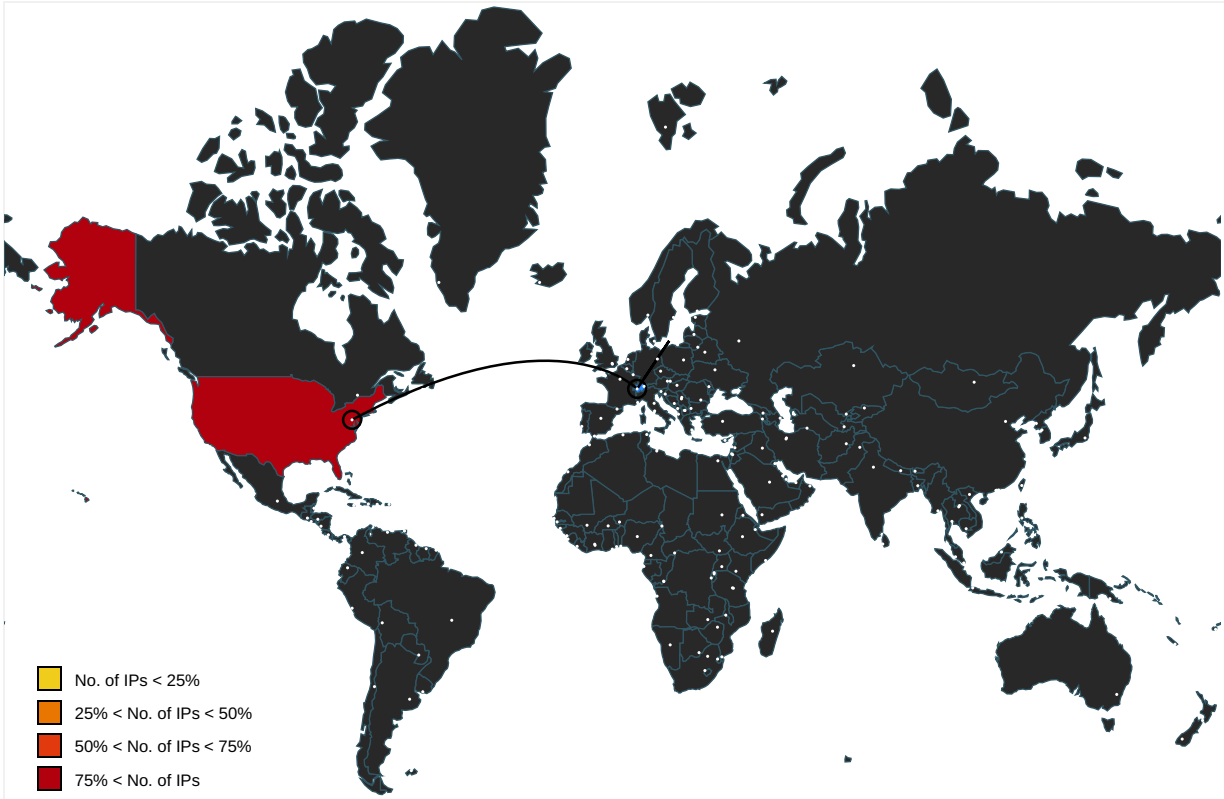
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49560412 4.00000000030D1000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.carterandcone.comn-u	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23122625 7.0000000005FA1000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49624838 7.00000000031A0000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.tiro.com	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.fontbureau.comessed	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23477786 6.0000000005F82000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comuec	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23502338 9.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23117215 1.0000000005FA1000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25115051 0.0000000002F26000.00000004.00 000001.sdmp	false		high
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n-u	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23173587 3.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/l	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23242732 2.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23418718 1.0000000005F82000.00000004.00 000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23230258 1.0000000005F82000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comml	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.24968281 8.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23402746 1.0000000005FA1000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25115051 0.0000000002F26000.00000004.00 000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/r-e	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23201354 4.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23238209 0.0000000005FA1000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23418718 1.0000000005F82000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25188345 2.0000000004116000.00000004.00 000001.sdmp, SecuriteInfo.com. Win32.32289.exe, 00000006.0000 0002.491127410.000000000040200 0.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// crt.sectigo.com/SectigoRSADomainValidationSecureServerCA .crt0#	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49624838 7.00000000031A0000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23410594 2.0000000005F82000.00000004.00 000001.sdmp, SecuriteInfo.com. Win32.32289.exe, 00000000.0000 0003.235609035.0000000005F8200 0.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49560412 4.00000000030D1000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com_	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23111904 9.0000000005FA0000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/y	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23406526 6.0000000005FA1000.00000004.00 000001.sdmp	false		high
http://https://sectigo.com/CPS0	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49624838 7.00000000031A0000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23173587 3.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49560412 4.00000000030D1000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd~	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23477786 6.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comic	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23410594 2.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/R	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23201354 4.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgretaw	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23424579 4.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdw	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23477786 6.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.privateemail.com	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49624838 7.00000000031A0000.00000004.00 000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23242732 2.0000000005F82000.00000004.00 000001.sdmp, SecuriteInfo.com. Win32.32289.exe, 00000000.0000 0003.232358854.0000000005F8200 0.00000004.00000001.sdmp, Secu riteInfo.com.Win32.32289.exe, 00000000.00000003.232302581.00 00000005F82000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23588777 1.0000000005F82000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com-d	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23117215 1.0000000005FA1000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/w	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23242732 2.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23513286 9.0000000005F7C000.00000004.00 000001.sdmp, SecuriteInfo.com. Win32.32289.exe, 00000000.0000 0002.255309143.000000000606000 0.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/_	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23410594 2.0000000005F82000.00000004.00 000001.sdmp	false		high
http://www.fontbureau.comdR	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23464224 6.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comoitu	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23560903 5.0000000005F82000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comcomF	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23560903 5.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.c/	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.50030229 2.0000000006E40000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comas2	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.24968281 8.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23242732 2.0000000005F82000.00000004.00 000001.sdmp, SecuriteInfo.com. Win32.32289.exe, 00000000.0000 0003.231891284.0000000005F8200 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23424579 4.0000000005F82000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.32289.exe, 00000000.00000002.25530914 3.0000000006060000.00000002.00 000001.sdmp	false		high
http://www.fontbureau.comdsed	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23477786 6.0000000005F82000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mFCOAY.com	SecuriteInfo.com.Win32.32289.exe, 00000006.00000002.49560412 4.00000000030D1000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalic	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23560903 5.0000000005F82000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers:	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23443700 2.0000000005FA1000.00000004.00 000001.sdmp	false		high
http://www.tiro.comic	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23148189 0.0000000005FA2000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deoi6Y	SecuriteInfo.com.Win32.32289.exe, 00000000.00000003.23402746 1.0000000005FA1000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.122.60	unknown	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356595
Start date:	23.02.2021
Start time:	11:52:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.32289.26241 (renamed file extension from 26241 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@6/4@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 60.7% • Quality standard deviation: 3.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.104.144.132, 131.253.33.200, 13.107.22.200, 13.64.90.137, 168.61.161.212, 104.43.139.144, 92.122.145.220, 184.30.20.56, 13.88.21.125, 8.248.117.254, 8.253.207.120, 8.253.204.121, 8.248.147.254, 67.26.75.254, 51.103.5.186, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
11:53:52	API Interceptor	774x Sleep call for process: SecuriteInfo.com.Win32.32289.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	SecuriteInfo.com.Win32.18332.exe	Get hash	malicious	Browse	
	s3HAoqkLuR.exe	Get hash	malicious	Browse	
	Request For Quotation RFQ 53253quote Pricelist of Order.doc	Get hash	malicious	Browse	
	Order Specification.doc	Get hash	malicious	Browse	
	ORDER.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.FileRepMalware.4966.exe	Get hash	malicious	Browse	
	dwXuNeEeql.exe	Get hash	malicious	Browse	
	DG6PQDuCfL.exe	Get hash	malicious	Browse	
	KlvNqu5mwX.exe	Get hash	malicious	Browse	
	tBNZZd447N.exe	Get hash	malicious	Browse	
	b31cHqumvH.exe	Get hash	malicious	Browse	
	O65XH93Hl6.exe	Get hash	malicious	Browse	
	ZbnDULcjzp.exe	Get hash	malicious	Browse	
	pDFkpNZVB7.exe	Get hash	malicious	Browse	
	ztoq7ir7cm.exe	Get hash	malicious	Browse	
	1r7gZ8xeDL.exe	Get hash	malicious	Browse	
	RFQ-21123.doc	Get hash	malicious	Browse	
	Inquiry.doc	Get hash	malicious	Browse	
	PO2172021.doc	Get hash	malicious	Browse	
	5043-200 Project TC Rev.0..doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	SecuriteInfo.com.Win32.18332.exe	Get hash	malicious	Browse	• 198.54.122.60
	s3HAoqkLuR.exe	Get hash	malicious	Browse	• 198.54.122.60
	Request For Quotation RFQ 53253quote Pricelist of Order.doc	Get hash	malicious	Browse	• 198.54.122.60
	Order Specification.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.FileRepMalware.4966.exe	Get hash	malicious	Browse	• 198.54.122.60
	dwXuNeEeql.exe	Get hash	malicious	Browse	• 198.54.122.60
	DG6PQDuCfL.exe	Get hash	malicious	Browse	• 198.54.122.60
	KlvNqu5mwX.exe	Get hash	malicious	Browse	• 198.54.122.60
	tBNZZd447N.exe	Get hash	malicious	Browse	• 198.54.122.60
	b31cHqumvH.exe	Get hash	malicious	Browse	• 198.54.122.60
	O65XH93Hl6.exe	Get hash	malicious	Browse	• 198.54.122.60
	ZbnDULcjzp.exe	Get hash	malicious	Browse	• 198.54.122.60
	pDFkpNZVB7.exe	Get hash	malicious	Browse	• 198.54.122.60
	ztoq7ir7cm.exe	Get hash	malicious	Browse	• 198.54.122.60
	1r7gZ8xeDL.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ-21123.doc	Get hash	malicious	Browse	• 198.54.122.60
	Inquiry.doc	Get hash	malicious	Browse	• 198.54.122.60
	PO2172021.doc	Get hash	malicious	Browse	• 198.54.122.60
	5043-200 Project TC Rev.0..doc	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	SecuriteInfo.com.Win32.18332.exe	Get hash	malicious	Browse	• 198.54.122.60
	s3HAoqkLuR.exe	Get hash	malicious	Browse	• 198.54.122.60
	KS8siMUTE5e1x6h.exe	Get hash	malicious	Browse	• 192.64.119.253
	proposal.xlsm	Get hash	malicious	Browse	• 198.54.116.171
	Request For Quotation RFQ 53253quote Pricelist of Order.doc	Get hash	malicious	Browse	• 198.54.122.60
	NewOrder.xlsm	Get hash	malicious	Browse	• 198.54.115.38
	mexhlc.xlsx	Get hash	malicious	Browse	• 199.188.20 0.203
	Order Specification.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER.doc	Get hash	malicious	Browse	• 198.54.122.60
	Order83930.exe	Get hash	malicious	Browse	• 198.54.117.210

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	receipt145.htm	Get hash	malicious	Browse	• 198.54.115.226
	SecuriteInfo.com.Trojan.Inject4.6572.1327.exe	Get hash	malicious	Browse	• 162.213.253.52
	SecuriteInfo.com.FileRepMalware.4966.exe	Get hash	malicious	Browse	• 198.54.122.60
	eInvoice.exe	Get hash	malicious	Browse	• 198.54.117.215
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 198.54.117.218
	Outstanding Invoices.pdf.exe	Get hash	malicious	Browse	• 199.192.19.85
	SecuriteInfo.com.W32.AIDetectGBM.malware.01.25871.exe	Get hash	malicious	Browse	• 162.0.235.69
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• 198.187.29.8
	BANK SWIFT- USD 98,712.00.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	urgent specification request.exe	Get hash	malicious	Browse	• 162.0.232.231

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\avJawOiuQtyAB.exe	Request For Quotation RFQ 53253quote Pricelist of Order.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.32289.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Local\Temp\tmp7060.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.176583403973694
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBBrtn:cbhH7MlNQ8/rydbz9I3YODOLNdq39
MD5:	D1A16AA2546C31AF2B84B6C80C6FB190
SHA1:	9424A2EAC962E951AF770470A47FA9653C1146FD
SHA-256:	16123AFF9C223C4B0E1AD9950C9945C1F5E4CCE6C12F0EE8B4ECBC6F7BD5F91A
SHA-512:	59FB19F19109F30C491ADA22773F1723E52F93C129FECA11AA83A33B522E26750AA6524DCD8D14D7E8B3527D1D6F809D7EE216A1E2D3BF892EEC1D79F51D21D
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp7060.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\avJawOiuQtyAB.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	523264
Entropy (8bit):	7.48125985477993
Encrypted:	false
SSDEEP:	12288:IZq4gLdN25pVrMgxv4XlmDCD1UmG5B3J91m6tUpHWv7TtnGY3:mpSgi3DXG5B3HUKv7JGG
MD5:	C59F71A02C13A01D95BF37C095895748
SHA1:	59C60B6A90CEC4676AFCC55A1397409E9D54B792
SHA-256:	983C358590898925DB49D1D6A731B54D37C76760267664BE45A7DC00646CFF60
SHA-512:	F3CE51DFAEFB5CA303C9FACF646581AF0CA7E823A0BC1F13BBD927A394BA701A82A5D188726FB6C6471928D1D2469B499654520FB5EADF264F8D0B49CD5059 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Joe Sandbox View:	• Filename: Request For Quotation RFQ 53253quote Pricelist of Order.doc, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...QG4`.....P..... ... ....@.. .....`..... ..@.....L...O.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....x..dS.....@9.....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*N..(. ...o....(&....*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<..... ...~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\avJawOiuQtyAB.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.48125985477993
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.Win32.32289.exe
File size:	523264

General

MD5:	c59f71a02c13a01d95bf37c095895748
SHA1:	59c60b6a90cec4676afcc55a1397409e9d54b792
SHA256:	983c358590898925db49d1d6a731b54d37c76760267664be45a7dc00646cff60
SHA512:	f3ce51dfaefb5ca303c9facf646581af0ca7e823a0bc1f13bbd927a394ba701a82a5d188726fb6c6471928d1d2469b499654520fb5eadf264f8d0b49cd5059a0
SSDEEP:	12288:IZq4gLdN25pVrMgxv4XlmDCD1UmG5B3J91m6tUpHWv7TtnGY3:mpSgi3DXG5B3HUKv7JGG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...QG4`.....P..... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48059e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60344751 [Tue Feb 23 00:07:45 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8054c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x1018	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x84000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7e5a4	0x7e600	False	0.770962768917	XENIX 8086 relocatable or 80286 small model	7.49673796579	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x1018	0x1200	False	0.360026041667	data	4.71751017087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x84000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x82090	0x364	data		
RT_MANIFEST	0x82404	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

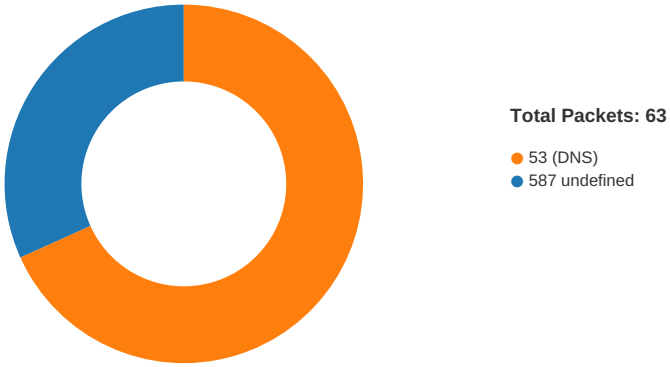
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	IndexOutOfRangeException.exe
FileVersion	1.0.0.0
CompanyName	

Description	Data
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	IndexOutOfRangeException.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:55:28.918190002 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:29.114044905 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.114223003 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:29.309323072 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.309783936 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:29.504745960 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.504995108 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.505373955 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:29.698975086 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.739454031 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:29.933242083 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.934806108 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.934828043 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.934842110 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.934859991 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:29.934995890 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:29.935026884 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:29.967792034 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:30.161506891 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:30.162404060 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:30.210645914 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:30.280126095 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:30.473779917 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:30.474215984 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:30.476454973 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:30.670069933 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:30.671242952 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:30.672158003 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:30.867106915 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:30.868954897 CET	587	49752	198.54.122.60	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:55:30.870229959 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:31.066046953 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.068936110 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.069305897 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:31.264831066 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.298664093 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.301223993 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:31.494898081 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.495676041 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.499644041 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:31.500041962 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:31.500201941 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:31.500412941 CET	49752	587	192.168.2.7	198.54.122.60
Feb 23, 2021 11:55:31.693182945 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.693484068 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.693598032 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.693841934 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.744534969 CET	587	49752	198.54.122.60	192.168.2.7
Feb 23, 2021 11:55:31.784375906 CET	49752	587	192.168.2.7	198.54.122.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:53:37.324696064 CET	56590	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:37.346414089 CET	60501	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:37.398123026 CET	53	60501	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:37.398149014 CET	53	56590	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:37.924494982 CET	53775	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:37.976074934 CET	53	53775	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:39.187776089 CET	51837	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:39.236498117 CET	53	51837	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:40.237482071 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:40.288151026 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:41.169795036 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:41.220515013 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:41.344861031 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:41.401891947 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:42.295595884 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:42.344197035 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:43.674968004 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:43.732306957 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:56.420617104 CET	58717	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:56.481400013 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:57.417709112 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:57.466243029 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 11:53:58.803383112 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:53:58.853167057 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:01.059923887 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:01.108777046 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:02.928941965 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:02.977508068 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:03.519138098 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:03.580275059 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:04.018068075 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:04.075110912 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:05.369021893 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:05.418167114 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:06.354378939 CET	52816	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:06.405890942 CET	53	52816	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:07.593808889 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:07.645380974 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:08.745326996 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:08.797349930 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:11.753947973 CET	54911	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:54:11.802594900 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:13.056674957 CET	49958	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:13.115480900 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:14.085145950 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:14.136672020 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:15.077722073 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:15.134660006 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:15.625641108 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:15.674793005 CET	53	59730	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:16.145185947 CET	59310	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:16.196734905 CET	53	59310	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:33.575124025 CET	51919	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:33.617065907 CET	64296	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:33.623955965 CET	53	51919	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:33.665894985 CET	53	64296	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:35.970069885 CET	56680	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:36.018896103 CET	53	56680	8.8.8.8	192.168.2.7
Feb 23, 2021 11:54:45.529062033 CET	58820	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:54:45.592629910 CET	53	58820	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:04.665044069 CET	60983	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:04.728240013 CET	53	60983	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:05.443793058 CET	49247	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:05.500611067 CET	52286	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:05.500899076 CET	53	49247	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:05.573424101 CET	53	52286	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:06.090641022 CET	56064	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:06.176846981 CET	53	56064	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:06.627093077 CET	63744	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:06.698909044 CET	53	63744	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:07.546226025 CET	61457	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:07.613472939 CET	53	61457	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:08.198966980 CET	58367	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:08.258806944 CET	53	58367	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:08.993110895 CET	60599	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:09.050955057 CET	53	60599	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:10.284003019 CET	59571	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:10.344754934 CET	53	59571	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:11.919641018 CET	52689	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:11.968408108 CET	53	52689	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:12.436631918 CET	50290	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:12.496738911 CET	53	50290	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:28.823223114 CET	60427	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:28.886399984 CET	53	60427	8.8.8.8	192.168.2.7
Feb 23, 2021 11:55:38.026177883 CET	56209	53	192.168.2.7	8.8.8.8
Feb 23, 2021 11:55:38.074975967 CET	53	56209	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 11:55:28.823223114 CET	192.168.2.7	8.8.8.8	0xc5c	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 11:55:28.886399984 CET	8.8.8.8	192.168.2.7	0xc5c	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

SMTP Packets

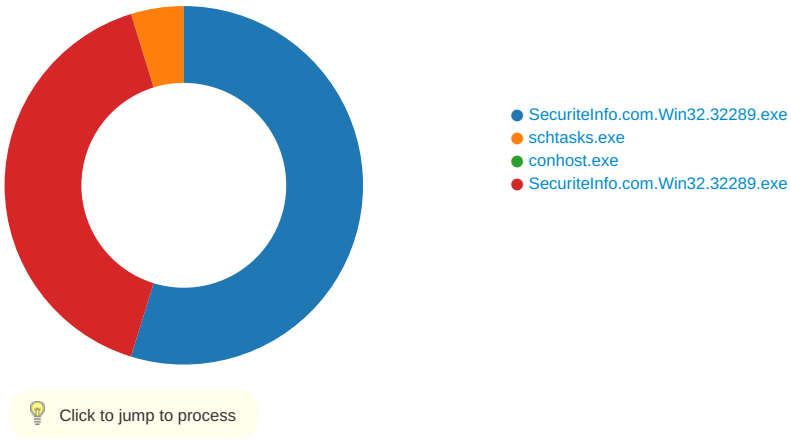
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 11:55:29.309323072 CET	587	49752	198.54.122.60	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 23, 2021 11:55:29.309783936 CET	49752	587	192.168.2.7	198.54.122.60	EHLO 549163

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 11:55:29.504995108 CET	587	49752	198.54.122.60	192.168.2.7	250-mta-11.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 23, 2021 11:55:29.505373955 CET	49752	587	192.168.2.7	198.54.122.60	STARTTLS
Feb 23, 2021 11:55:29.698975086 CET	587	49752	198.54.122.60	192.168.2.7	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.32289.exe PID: 6228 Parent PID: 5572

General

Start time:	11:53:44
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe'
Imagebase:	0xb40000
File size:	523264 bytes
MD5 hash:	C59F71A02C13A01D95BF37C095895748
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.251883452.0000000004116000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.251150510.0000000002F26000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.251021706.0000000002EA1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D39CF06	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	6D39CF06	unknown
C:\Users\user\AppData\Roaming\avJawOiuQtyAB.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	6C1EDD66	CopyFileW
C:\Users\user\AppData\Roaming\avJawOiuQtyAB.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C1EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7060.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1E7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.32289.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6AC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7060.tmp	success or wait	1	6C1E6A95	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\avJawOiuQtyAB.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 51 47 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e6 07 00 00 14 00 00 00 00 00 00 9e 05 08 00 00 20 00 00 00 20 08 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 60 08 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L...QG4`.......... ....P................. ... ....@.. ......................` ....@................	success or wait	4	6C1EDD66	CopyFileW
C:\Users\user\AppData\Roaming\avJawOiuQtyAB.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	6C1EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7060.tmp	unknown	1662	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6C1E1B4F	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.Win32.32289.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6AC907	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	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1E1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6444 Parent PID: 6228

General

Start time:	11:53:54
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\avJawOiuQtyAB' /XML 'C:\Users\user\AppData\Local\Temp\tmp7060.tmp'
Imagebase:	0x330000
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\tmp7060.tmp	unknown	2	success or wait	1	33AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7060.tmp	unknown	1663	success or wait	1	33ABD9	ReadFile

Analysis Process: conhost.exe PID: 6460 Parent PID: 6444

General

Start time:	11:53:54
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuriteInfo.com.Win32.32289.exe PID: 6496 Parent PID: 6228

General

Start time:	11:53:54
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.32289.exe
Imagebase:	0xc10000
File size:	523264 bytes
MD5 hash:	C59F71A02C13A01D95BF37C095895748
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.495792396.0000000003112000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.495604124.00000000030D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.495604124.00000000030D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.491127410.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D39CF06	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	6D39CF06	unknown

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	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1E1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1E1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1E1B4F	ReadFile

Disassembly

Code Analysis