ID: 339176
Sample Name:
SecuriteInfo.com.BehavesLike.Win32.Generic.cc.14146
Cookbook: default.jbs
Time: 16:43:34
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

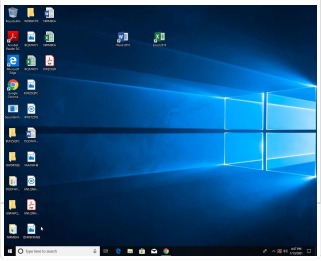
Analysis Report SecuriteInfo.com.BehavesLike.Win32.G…

Overview

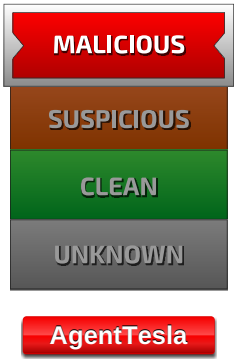
General Information

Sample Name:	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.14146 (renamed file extension from 14146 to exe)
Analysis ID:	339176
MD5:	b232b5c7754d93..
SHA1:	7c3d92552f6ebab.
SHA256:	3311cea59262b0..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

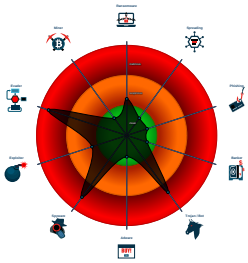


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe (PID: 7164 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe' MD5: B232B5C7754D932B07C0D47F934EFBFE)
  - SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe (PID: 6108 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe MD5: B232B5C7754D932B07C0D47F934EFBFE)
  - SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe (PID: 3152 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe MD5: B232B5C7754D932B07C0D47F934EFBFE)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "=0AGywGPT",
  "URL: ": "https://wV71njTiOcKvohmw.org",
  "To: ": "0012@dividekings.com",
  "ByHost: ": "smtp.privateemail.com:587",
  "Password: ": "qOQRsCQgut",
  "From: ": "0012@dividekings.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.998174021.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.667526468.0000000003A49000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.666339476.0000000002A41000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.999750695.000000000308 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe PID: 7164	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

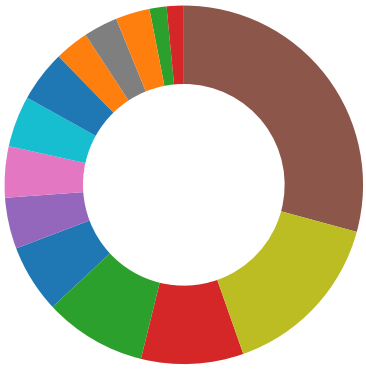
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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 submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

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)

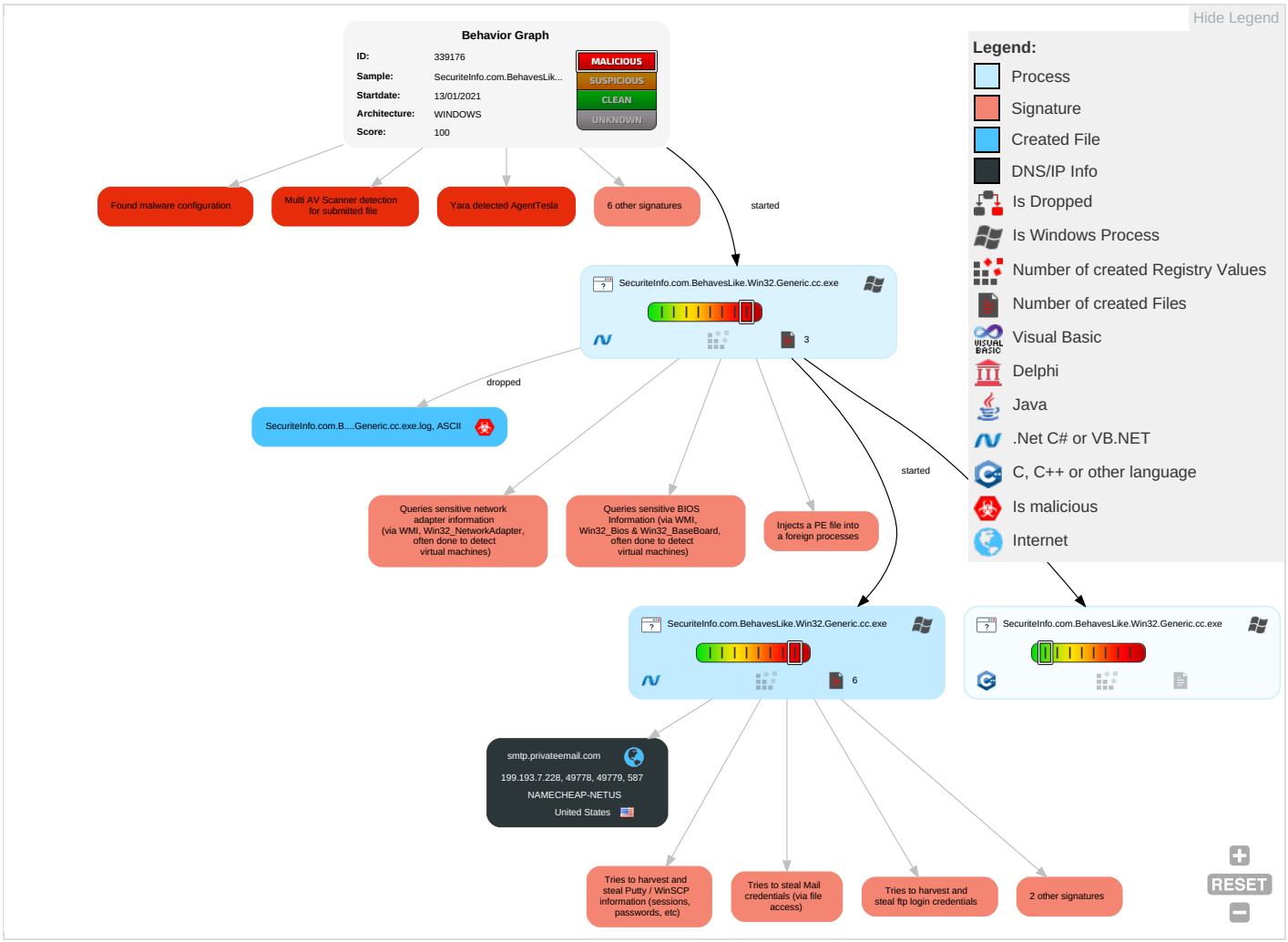
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Input Capture 1 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-S Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-A Layer
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Appli Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallba Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Port

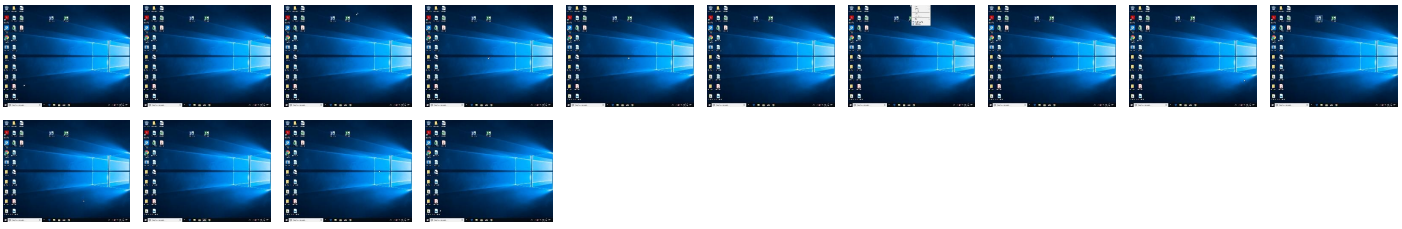
Behavior Graph



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.BehavesLike.Win32.Generic.cc.exe	20%	ReversingLabs	Win32.Trojan.Generic	
SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://wV71njTiOcKvohmw.org	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://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://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://MLrjrg.com	0%	Avira URL Cloud	safe	
http://ocsp.use3	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.privateemail.com	199.193.7.228	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://wV71njTiOcKvohmw.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.1000561645.00000000033EE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.999750695.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.999750695.0000000003081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.1000561645.00000000033EE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.1000561645.00000000033EE000.00000004.00000001.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%tordir%%ha	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.999750695.0000000003081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%GETMozilla/5.0	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.999750695.0000000003081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://MLrjrg.com	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.999750695.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.use3	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.998907100.0000000001433000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.999750695.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000000.00000002.667526468.0000000003A49000.00000004.00000001.sdmp, SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.998174021.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.privateemail.com	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe, 00000003.00000002.1000561645.00000000033EE000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond

Analysis ID:	339176
Start date:	13.01.2021
Start time:	16:43:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.14146 (renamed file extension from 14146 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:	19
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@5/2@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.8% (good quality ratio 3.8%) • Quality average: 71% • Quality standard deviation: 0%
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): BackgroundTransferHost.exe, wermgr.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.64.90.137, 51.104.139.180, 40.88.32.150, 92.122.213.194, 92.122.213.247, 8.253.204.120, 8.253.95.249, 67.27.159.254, 67.27.233.254, 8.248.149.254, 20.54.26.129, 52.155.217.156, 20.190.129.130, 20.190.129.19, 40.126.1.145, 40.126.1.128, 40.126.1.130, 20.190.129.133, 20.190.129.24, 20.190.129.17, 52.147.198.201, 51.104.144.132 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, login.msa.msidentity.com, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339176/sample/SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe

Simulations

Behavior and APIs

Time	Type	Description
16:44:28	API Interceptor	1052x Sleep call for process: SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.193.7.228	DHL-Address.xlsx	Get hash	malicious	Browse	
	shipping-document.xlsx	Get hash	malicious	Browse	
	iVUeQOg6LO.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	
	DHL-document.xlsx	Get hash	malicious	Browse	
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	
	Mj1eX5GWJxDRnuk.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Inject4.6535.8815.exe	Get hash	malicious	Browse	
	shipping document.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6512.28917.exe	Get hash	malicious	Browse	
	p72kooG5ak.exe	Get hash	malicious	Browse	
	additional items.xlsx	Get hash	malicious	Browse	
	swift copy 1f354972.exe	Get hash	malicious	Browse	
	DB_DHL_AWB_00117980920AD.exe	Get hash	malicious	Browse	
	Payment Advice - Advice Ref[G20376302776].pptx.exe	Get hash	malicious	Browse	
	Payment Reminder & SOA 202020121158.exe	Get hash	malicious	Browse	
	kg.exe	Get hash	malicious	Browse	
	logo.exe	Get hash	malicious	Browse	
	Pictures.exe	Get hash	malicious	Browse	
	7iZX0KCH4C.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.privateemail.com	DHL-Address.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	Mj1eX5GWJxDRnuk.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6535.8815.exe	Get hash	malicious	Browse	• 199.193.7.228
	shipping document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6512.28917.exe	Get hash	malicious	Browse	• 199.193.7.228
	p72kooG5ak.exe	Get hash	malicious	Browse	• 199.193.7.228
	additional items.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	swift copy 1f354972.exe	Get hash	malicious	Browse	• 199.193.7.228
	DB_DHL_AWB_00117980920AD.exe	Get hash	malicious	Browse	• 199.193.7.228
	Payment Advice - Advice Ref[G20376302776].pptx.exe	Get hash	malicious	Browse	• 199.193.7.228
	Payment Reminder & SOA 202020121158.exe	Get hash	malicious	Browse	• 199.193.7.228
	kg.exe	Get hash	malicious	Browse	• 199.193.7.228
	logo.exe	Get hash	malicious	Browse	• 199.193.7.228
	Pictures.exe	Get hash	malicious	Browse	• 199.193.7.228
	PO48905232020.exe	Get hash	malicious	Browse	• 199.193.7.228

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	DHL-Address.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	New FedEx paper work review.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO-000202112.exe	Get hash	malicious	Browse	• 63.250.34.114
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 162.255.118.194
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order -263.exe	Get hash	malicious	Browse	• 162.0.232.59
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 162.255.119.136
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 162.0.238.245
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Invoice.exe	Get hash	malicious	Browse	• 162.213.255.55
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 68.65.122.35
	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 198.54.125.162

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\jebez5tq.lzt\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.300736524263088

General

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.BehavesLike.Win32.Generic.cc.exe
File size:	843776
MD5:	b232b5c7754d932b07c0d47f934efbfe
SHA1:	7c3d92552f6ebab8956727beecaac5d22c87a55b
SHA256:	3311cea59262b019a69fb72b72a36fc8e55d48a0f14f853b3a52fc8740542e99
SHA512:	4e3abe570fa413fb74b1efcf56560d5275cbcaf8217779e46dc65e13c2185c23f0be2b01b91dcb5aead24c6f68e8f84b432b7efba87f2cc835bfa2848a406740
SSDEEP:	12288:8XT4rp65D+SL7y7INIIdGZMonTVA2Wsa8tpJKS:VhSJNILZn62WJ8td
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....>.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cf43e
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:	0x5FFEB6D9 [Wed Jan 13 09:01:13 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

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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xcf3ec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0x5c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	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	0xcd444	0xcd600	False	0.697408275639	data	7.3067407255	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x5c4	0x600	False	0.421875	data	4.12609636513	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd0090	0x334	data		
RT_MANIFEST	0xd03d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

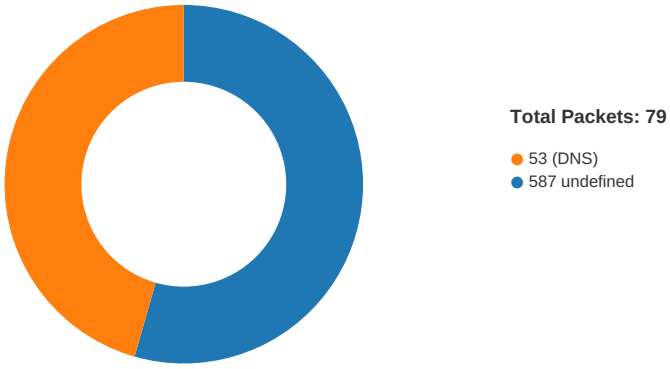
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011
Assembly Version	1.0.0.0
InternalName	DESCUNION.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	FileReplacement
ProductVersion	1.0.0.0
FileDescription	FileReplacement
OriginalFilename	DESCUNION.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:46:11.757272005 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:11.948328018 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:11.948523998 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:12.142493963 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.142971039 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:12.333554983 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.333998919 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.334683895 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:12.525620937 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.566602945 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:12.609807968 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:12.800419092 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.802321911 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.802376986 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.802535057 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:12.802803040 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:12.847980976 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:12.993083954 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.036071062 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:13.226752043 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.227642059 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.227680922 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.227817059 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:13.500853062 CET	49778	587	192.168.2.4	199.193.7.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:46:13.691303015 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.697016001 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.698837996 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:13.889292002 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.895484924 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:13.896471977 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.087001085 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.090814114 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.091847897 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.282464981 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.283643007 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.284425974 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.474961042 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.507121086 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.507625103 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.698227882 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.699042082 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.701308966 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.701559067 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.702471972 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.702558994 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:14.891746044 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.891773939 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.892991066 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.893054962 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.904805899 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:14.957734108 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:16.780534983 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:16.971262932 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:16.971898079 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:16.971944094 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:16.972031116 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:17.930212021 CET	49778	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:18.120556116 CET	587	49778	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:18.413789988 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:18.604154110 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:18.604260921 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:18.802757025 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:18.803105116 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:18.993189096 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:18.993951082 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:18.994271994 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:19.184335947 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.185312986 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:19.375399113 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.375586033 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.375633955 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.375828028 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:19.378537893 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:19.380388975 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:19.568555117 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.568856001 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.570337057 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.570744991 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.571544886 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:19.761825085 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.762775898 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:19.764028072 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:20.067236900 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:20.411036015 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:20.960117102 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:20.960897923 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:21.150852919 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:21.157138109 CET	587	49779	199.193.7.228	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:46:21.157592058 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:21.347753048 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:21.380951881 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:21.381484985 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:21.571430922 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:21.574239016 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:21.576109886 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:21.576283932 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:21.576421022 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:21.576558113 CET	49779	587	192.168.2.4	199.193.7.228
Jan 13, 2021 16:46:21.766364098 CET	587	49779	199.193.7.228	192.168.2.4
Jan 13, 2021 16:46:21.766382933 CET	587	49779	199.193.7.228	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:44:17.688914061 CET	64549	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:17.737062931 CET	53	64549	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:18.491009951 CET	63153	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:18.538971901 CET	53	63153	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:19.322529078 CET	52991	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:19.370450974 CET	53	52991	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:20.486376047 CET	53700	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:20.534308910 CET	53	53700	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:21.909039021 CET	51726	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:21.957000017 CET	53	51726	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:22.688029051 CET	56794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:22.744488955 CET	53	56794	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:23.588207960 CET	56534	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:23.636066914 CET	53	56534	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:24.724006891 CET	56627	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:24.774846077 CET	53	56627	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:25.591173887 CET	56621	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:25.641993999 CET	53	56621	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:26.984771013 CET	63116	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:27.033406973 CET	53	63116	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:29.066828012 CET	64078	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:29.117539883 CET	53	64078	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:46.950552940 CET	64801	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:46.998497963 CET	53	64801	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:50.241781950 CET	61721	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:50.289705992 CET	53	61721	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:51.028373957 CET	51255	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:51.079880953 CET	53	51255	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:51.862539053 CET	61522	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:51.913247108 CET	53	61522	8.8.8.8	192.168.2.4
Jan 13, 2021 16:44:52.190464020 CET	52337	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:44:52.247957945 CET	53	52337	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:07.352602005 CET	55046	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:07.400609970 CET	53	55046	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:07.570275068 CET	49612	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:07.618177891 CET	53	49612	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:10.204570055 CET	49285	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:10.276086092 CET	53	49285	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:10.574723005 CET	50601	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:10.633799076 CET	53	50601	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:11.261090040 CET	60875	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:11.320754051 CET	53	60875	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:11.922899008 CET	56448	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:11.979140043 CET	53	56448	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:12.408426046 CET	59172	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:12.467674017 CET	53	59172	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:12.913372993 CET	62420	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:12.969984055 CET	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 16:45:13.490417957 CET	60579	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:13.547166109 CET	53	60579	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:14.096458912 CET	50183	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:14.152939081 CET	53	50183	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:14.992047071 CET	61531	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:15.051367998 CET	53	61531	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:15.886110067 CET	49228	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:15.946121931 CET	53	49228	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:16.387881994 CET	59794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:16.444397926 CET	53	59794	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:23.680166960 CET	55916	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:23.737891912 CET	53	55916	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:51.966533899 CET	52752	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:52.017374992 CET	53	52752	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:52.530791998 CET	60542	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:52.581692934 CET	53	60542	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:56.850696087 CET	60689	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:56.898529053 CET	53	60689	8.8.8.8	192.168.2.4
Jan 13, 2021 16:45:58.814208984 CET	64206	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:45:58.862072945 CET	53	64206	8.8.8.8	192.168.2.4
Jan 13, 2021 16:46:11.575026035 CET	50904	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:46:11.631670952 CET	53	50904	8.8.8.8	192.168.2.4
Jan 13, 2021 16:46:18.354671001 CET	57525	53	192.168.2.4	8.8.8.8
Jan 13, 2021 16:46:18.411058903 CET	53	57525	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 16:46:11.575026035 CET	192.168.2.4	8.8.8.8	0xeba4	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 13, 2021 16:46:18.354671001 CET	192.168.2.4	8.8.8.8	0xeef1	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 16:45:52.017374992 CET	8.8.8.8	192.168.2.4	0x49b6	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 16:46:11.631670952 CET	8.8.8.8	192.168.2.4	0xeba4	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 13, 2021 16:46:18.411058903 CET	8.8.8.8	192.168.2.4	0xeef1	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)

SMTP Packets

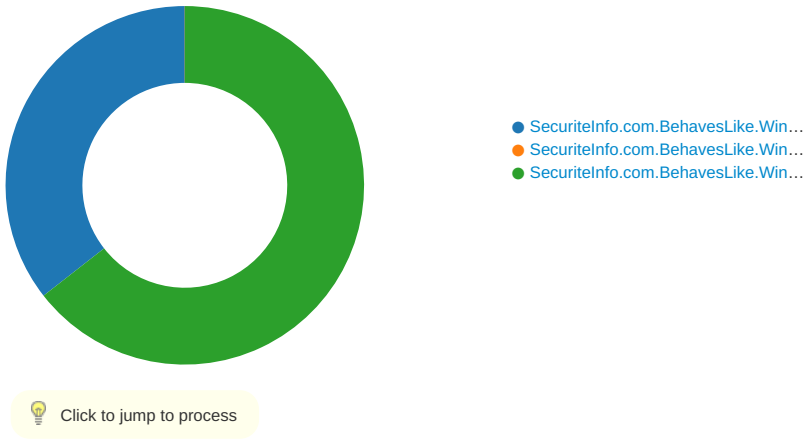
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 16:46:12.142493963 CET	587	49778	199.193.7.228	192.168.2.4	220 PrivateEmail.com Mail Node
Jan 13, 2021 16:46:12.142971039 CET	49778	587	192.168.2.4	199.193.7.228	EHLO 585948
Jan 13, 2021 16:46:12.333998919 CET	587	49778	199.193.7.228	192.168.2.4	250-MTA-06.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 13, 2021 16:46:12.334683895 CET	49778	587	192.168.2.4	199.193.7.228	STARTTLS
Jan 13, 2021 16:46:12.525620937 CET	587	49778	199.193.7.228	192.168.2.4	220 Ready to start TLS
Jan 13, 2021 16:46:18.802757025 CET	587	49779	199.193.7.228	192.168.2.4	220 PrivateEmail.com Mail Node
Jan 13, 2021 16:46:18.803105116 CET	49779	587	192.168.2.4	199.193.7.228	EHLO 585948

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 16:46:18.993951082 CET	587	49779	199.193.7.228	192.168.2.4	250-MTA-06.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 13, 2021 16:46:18.994271994 CET	49779	587	192.168.2.4	199.193.7.228	STARTTLS
Jan 13, 2021 16:46:19.184335947 CET	587	49779	199.193.7.228	192.168.2.4	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe PID: 7164
Parent PID: 5776

General

Start time:	16:44:22
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe'
Imagebase:	0x610000
File size:	843776 bytes
MD5 hash:	B232B5C7754D932B07C0D47F934EFBFE
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: 00000000.00000002.667526468.0000000003A49000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.666339476.0000000002A41000.00000004.00000001.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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe.log	unknown	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",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_v4.0.3	success or wait	1	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe PID: 6108 Parent PID: 7164

General

Start time:	16:44:29
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe
Imagebase:	0x40000
File size:	843776 bytes
MD5 hash:	B232B5C7754D932B07C0D47F934EFBFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe PID: 3152 Parent PID: 7164

General

Start time:	16:44:29
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe
Imagebase:	0xc70000
File size:	843776 bytes
MD5 hash:	B232B5C7754D932B07C0D47F934EFBFE
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: 00000003.00000002.998174021.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.999750695.0000000003081000.00000004.00000001.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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Roaming\jebez5tq.lzt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFCBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\jebez5tq.lzt\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFCBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\jebez5tq.lzt\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFCBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\jebez5tq.lzt\Chrome\Default\Cookies	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	6BFCDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jebez5tq.lzt\Chrome\Default\Cookies	success or wait	1	6BFC6A95	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\jebez5tq.lzt\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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 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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6BFCDD66	CopyFileW

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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\956ef416-cae9-40d1-9127-d1ae1c83dd55	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Roaming\jebez5tq.lzt\Chrome\Default\Cookies	unknown	16384	success or wait	2	6BFC1B4F	ReadFile

Disassembly

Code Analysis

Code Analysis