ID: 412370
Sample Name:
SecuriteInfo.com.Malware.AI.4228845530.13946.10796
Cookbook: default.jbs
Time: 16:46:33
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

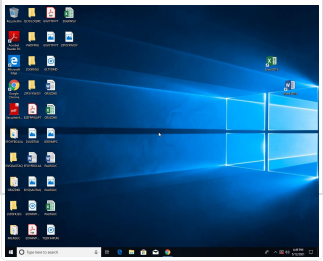
Analysis Report SecuriteInfo.com.Malware.AI.42288455…

Overview

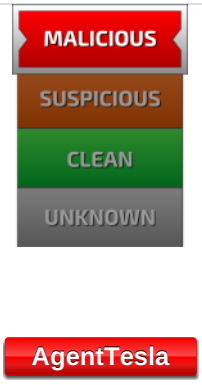
General Information

Sample Name:	SecuriteInfo.com.Malware.AI.4228845530.13946.10796 (renamed file extension from 10796 to exe)
Analysis ID:	412370
MD5:	248b7d11fab05df..
SHA1:	230f7982e0bcf4a..
SHA256:	778487cdb0077c..
Infos:	

Most interesting Screenshot:



Detection

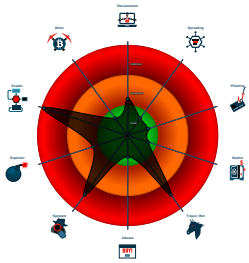


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- Contains functionality to check if a d…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- PE file contains section with special…
- PE file has nameless sections

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Malware.AI.4228845530.13946.exe (PID: 4012 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe' MD5: 248B7D11FAB05DF72C28B150AF6F2DD8)
  - SecuriteInfo.com.Malware.AI.4228845530.13946.exe (PID: 488 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe MD5: 248B7D11FAB05DF72C28B150AF6F2DD8)
  - SecuriteInfo.com.Malware.AI.4228845530.13946.exe (PID: 5596 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe MD5: 248B7D11FAB05DF72C28B150AF6F2DD8)
  - SecuriteInfo.com.Malware.AI.4228845530.13946.exe (PID: 5756 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe MD5: 248B7D11FAB05DF72C28B150AF6F2DD8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sergio.arroyo@kaeiser.comQIErWCn3smtp.kaeiser.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.502628732.000000000318 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000001.00000002.258294495.0000000002F8 3000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000006.00000002.498013758.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.498013758.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000001.00000002.260145188.0000000003F85000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

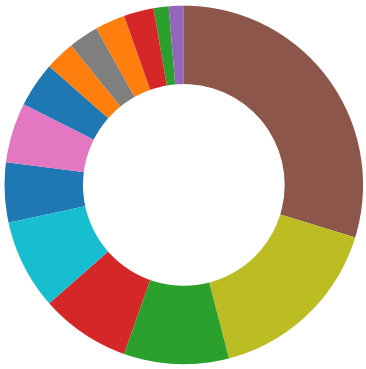
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.SecuriteInfo.com.Malware.AI.4228845530.13946.exe.4030b70.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.SecuriteInfo.com.Malware.AI.4228845530.13946.exe.4030b70.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.SecuriteInfo.com.Malware.AI.4228845530.13946.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.SecuriteInfo.com.Malware.AI.4228845530.13946.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.SecuriteInfo.com.Malware.AI.4228845530.13946.exe.4030b70.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

PE file contains section with special chars

PE file has nameless sections

Copyright Joe Security LLC 2021

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Yara detected AntiVM3

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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

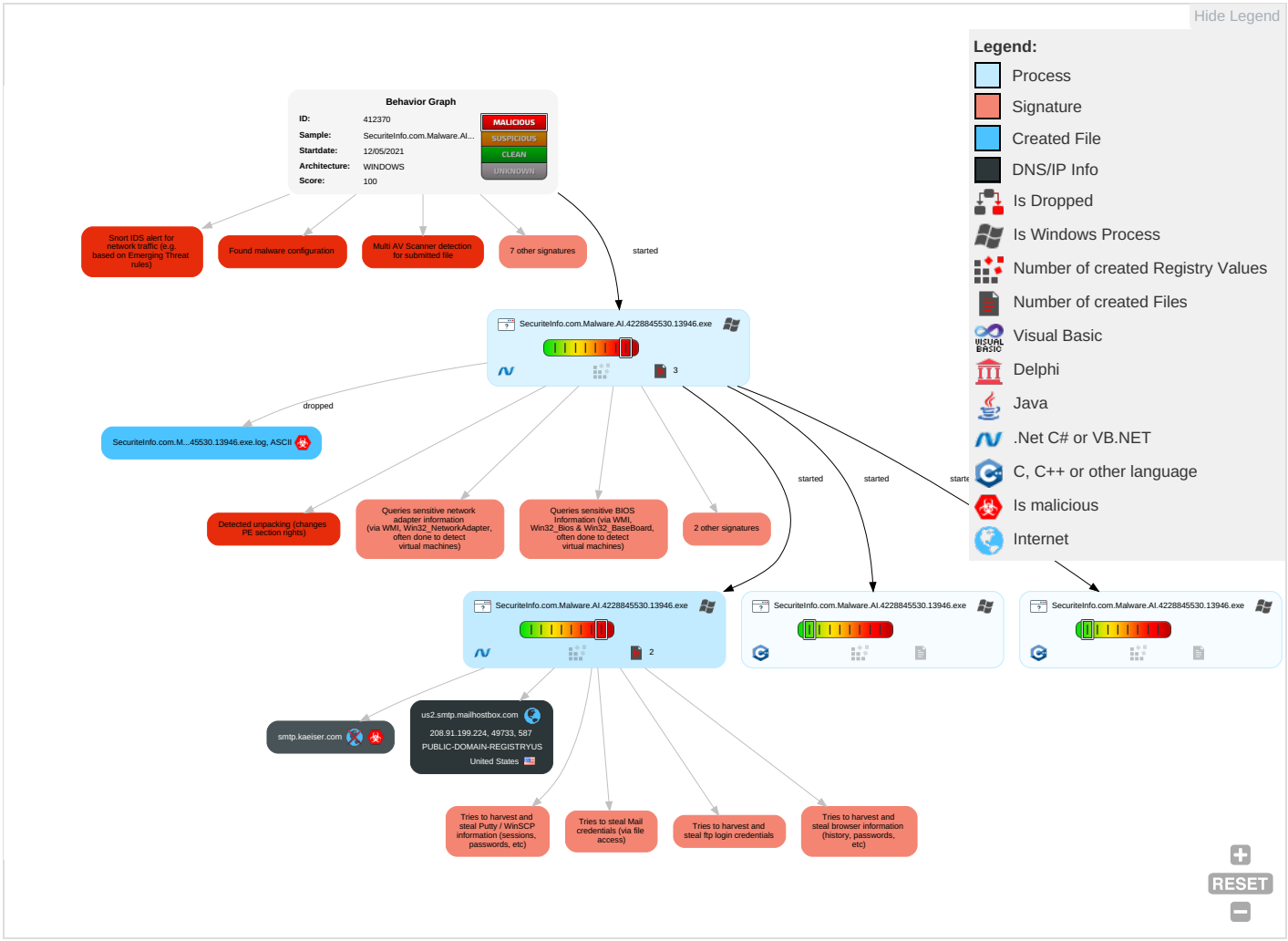
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Security Software Discovery 3 3 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 4 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used 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.Malware.AI.4228845530.13946.exe	32%	Virustotal		Browse
SecuriteInfo.com.Malware.AI.4228845530.13946.exe	36%	ReversingLabs	Win32.Trojan.Wacatac	
SecuriteInfo.com.Malware.AI.4228845530.13946.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.SecuriteInfo.com.Malware.AI.4228845530.13946.exe.a90000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.SecuriteInfo.com.Malware.AI.4228845530.13946.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.kaeiser.com	0%	Virustotal		Browse

URLs

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Virustotal		Browse
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://https://6JeA1hPBvojxA7lSjrqA.org4	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://https://6JeA1hPBvojxA7lSjrqA.org	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.html	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.htmlc	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://qdovFN.com	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/1	0%	Avira URL Cloud	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://smtp.kaeiser.com	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	
http://servermanager.miixit.org/downloads/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

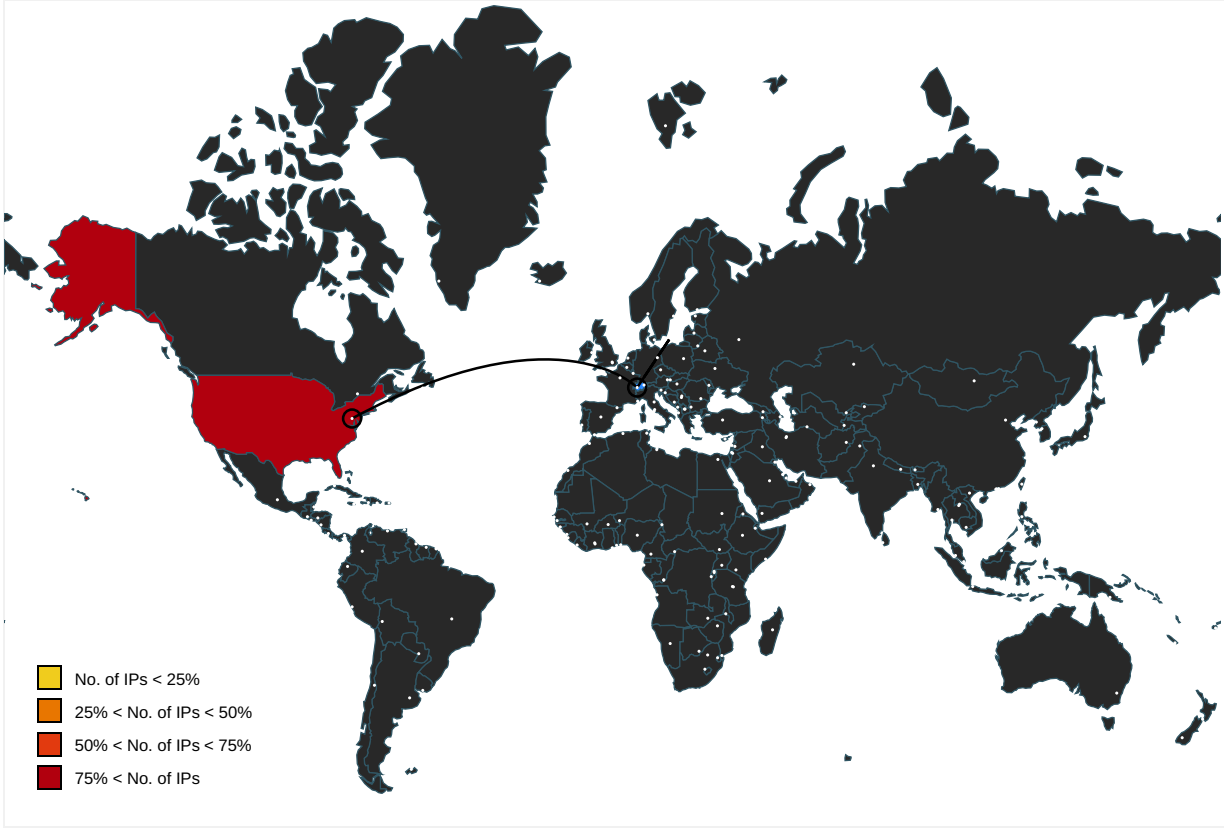
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high
smtp.kaeiser.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.502628732.000000003181000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.502628732.000000003181000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org/	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000003814000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://us2.smtp.mailhostbox.com	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.505677643.000000003431000.00000004.00000001.sdmp	false		high
http://https://6JeA1hPBvojxA7lSjrqA.org4	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.502628732.000000003181000.00000004.00000001.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.Malware.AI.4228845530.13946.exe, 00000006.00000002.502628732.000000003181000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://6JeA1hPBvojxA7lSjrqA.org	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.505339832.00000000033DF000.00000004.00000001.sdmp, SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000003.462075964.0000000001184000.00000004.00000001.sdmp, SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.505810185.0000000003440000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/index_ru.html	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.htmlc	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://qdovFN.com	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.502628732.0000000003181000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/1	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.502628732.0000000003181000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://smtp.kaeiser.com	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.505677643.0000000003431000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000002.258242489.0000000002F31000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000002.260145188.0000000003F85000.00000004.00000001.sdmp, SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.498013758.0000000000402000.00000040.00000001.sdmp	false	• 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.Malware.AI.4228845530.13946.exe, 00000001.00000002.258294495.0000000002F83000.00000004.00000001.sdmp	false		high
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC5servermana	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000001.00000003.248737778.000000000381A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	SecuriteInfo.com.Malware.AI.4228845530.13946.exe, 00000006.00000002.502628732.0000000003181000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412370
Start date:	12.05.2021
Start time:	16:46:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Malware.AI.4228845530.13946.10796 (renamed file extension from 10796 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@7/1@2/1
EGA Information:	Failed

Copyright Joe Security LLC 2021

HDC Information:	• Successful, ratio: 3.7% (good quality ratio 2%) • Quality average: 36.3% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 93.184.220.29, 104.42.151.234, 92.122.145.220, 104.43.193.48, 168.61.161.212, 184.30.20.56, 20.82.210.154, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, fs.microsoft.com, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:47:34	API Interceptor	669x Sleep call for process: SecuriteInfo.com.Malware.AI.4228845530.13946.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.224	PDF.9066721066.exe	Get hash	malicious	Browse	
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	
	Quotation..exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	QUOTATION ORDER.exe	Get hash	malicious	Browse	
	Request Sample products.exe	Get hash	malicious	Browse	
	Quotation RFQ8116300.exe	Get hash	malicious	Browse	
	New Enquiry 200567.exe	Get hash	malicious	Browse	
	7UKtv01ZdPSbdAD.exe	Get hash	malicious	Browse	
	Order Confirmation.exe	Get hash	malicious	Browse	
	Swift Copy.xlsx	Get hash	malicious	Browse	
	LM Approved Invoices 06052021.doc	Get hash	malicious	Browse	
	ADVICE84857584489393.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1STyZQU31dWqcMq.exe	Get hash	malicious	Browse	
	1g1NLI6i33.exe	Get hash	malicious	Browse	
	PO.xlsx	Get hash	malicious	Browse	
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	
	REQUEST FOR PRICE QUOTE - URGENT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	presupuesto.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 4500379537.exe	Get hash	malicious	Browse	• 208.91.199.225
	B5Cg5YZIzp.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 2345566 hisob-faktura.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation..exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Quotation..exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.224
	QUOTATION ORDER.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ_SGCCUP_24 590 34 532 -11052021.exe	Get hash	malicious	Browse	• 208.91.198.143
	Request Sample products.exe	Get hash	malicious	Browse	• 208.91.198.143
	QTY-3322.exe	Get hash	malicious	Browse	• 208.91.198.143
	Request Sample products.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Letter of Demand.doc	Get hash	malicious	Browse	• 103.21.59.173
	7b4NmGxyY2.exe	Get hash	malicious	Browse	• 162.215.24 1.145
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.22 5.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.22 5.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223
	bill 04050.xlsm	Get hash	malicious	Browse	• 103.21.59.208

JA3 Fingerprints

No context

Dropped Files

No context

Copyright Joe Security LLC 2021

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Malware.AI.4228845530.13946.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHR
MD5:	8198C64CE0786EABD4C792E7E6FC30E5
SHA1:	71E1676126F4616B18C751A0A775B2D64944A15A
SHA-256:	C58018934011086A883D1D56B21F6C1916B1CD83206ADD1865C9BDD29DADCBC4
SHA-512:	EE293C0F88A12AB10041F66DDFAE89BC11AB3B3AAD8604F1A418ABE43DF0980245C3B7F8FEB709AEE8E9474841A280E073EC063045EA39948E853AA6B4EC0FB0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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,"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..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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.76610281911688
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Malware.AI.4228845530.13946.exe
File size:	934400
MD5:	248b7d11fab05df72c28b150af6f2dd8
SHA1:	230f7982e0bcf4a0e1e164316d736101bc5b8d5e
SHA256:	778487cdb0077cbe811443b5247a8121c5fc7c7e23472c068eee1e41a1476745
SHA512:	52aade22e310127a1e4e809b2902b59cbd88de5b298cb17caa3c78ba39fa09bcc25187a63b8ed4d33d8d0060869a1f89c44d9e25cc51338a0b976083a5a900c5
SSDEEP:	24576:0bnpWiHvllK3sJecpFQDu4hV342SqtkFWhoTa9mmZ7:0bnUzQ+aDHV3aFWy6mmZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...,.`.....P.....|..... ....@.. .....@.....

File Icon

Icon Hash:	8a8ccae6e0fcc4aa

Static PE Info

General

Entrypoint:	0x4ea00a
Entrypoint Section:	
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:	0x609B842C [Wed May 12 07:30:52 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 [004EA000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc08dc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcc000	0x1b130	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	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	0xea000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xc0000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
sBa<03`	0x2000	0xbc6b8	0xbc800	False	1.00031861323	data	7.9997886445	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xc0000	0xbec0	0xc000	False	0.443725585938	data	5.98422695135	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x1b130	0x1b200	False	0.123334893433	data	3.48672876978	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xea000	0x10	0x200	False	0.044921875	dBase III DBT, version number 0, next free block index 788752	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xcc250	0x1b5f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xcddb0	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xde5d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xe2800	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xe4da8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xe5e50	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe62b8	0x5a	data		
RT_GROUP_ICON	0xe6314	0x14	data		
RT_VERSION	0xe6328	0x39c	data		
RT_MANIFEST	0xe66c4	0xa65	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 2013
Assembly Version	3.0.0.0
InternalName	IsolatedStorageSecurityOptions.exe
FileVersion	3.0.0.0
CompanyName	

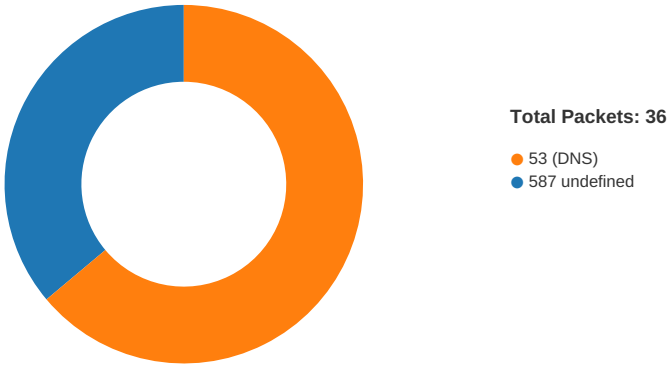
Description	Data
LegalTrademarks	
Comments	
ProductName	ServerManager_Core
ProductVersion	3.0.0.0
FileDescription	ServerManager_Core
OriginalFilename	IsolatedStorageSecurityOptions.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-16:49:21.211208	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49733	587	192.168.2.5	208.91.199.224

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:49:19.438030958 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:19.602700949 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:19.602816105 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:20.182816982 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:20.183258057 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:20.346558094 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:20.346596956 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:20.349409103 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:20.513592005 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:20.514242887 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:20.679681063 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:20.680565119 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:20.844995022 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:20.845446110 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:21.041570902 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:21.042124033 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:21.205835104 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:21.211208105 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:21.211504936 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:21.211669922 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:21.211858034 CEST	49733	587	192.168.2.5	208.91.199.224
May 12, 2021 16:49:21.374861002 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:21.375021935 CEST	587	49733	208.91.199.224	192.168.2.5
May 12, 2021 16:49:21.473221064 CEST	587	49733	208.91.199.224	192.168.2.5

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:49:21.525196075 CEST	49733	587	192.168.2.5	208.91.199.224

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:47:17.762149096 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 16:47:17.777302027 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:17.826127052 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 16:47:18.402791023 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:18.452846050 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 16:47:18.595149040 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:18.662967920 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 16:47:19.546247959 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:19.595191956 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 16:47:20.512152910 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:20.560919046 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 16:47:21.739219904 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:21.787822962 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 16:47:23.225873947 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:23.274524927 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 16:47:25.415198088 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:25.463933945 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 16:47:26.651551008 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:26.703161955 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 16:47:30.238341093 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:30.287147045 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 16:47:31.211246967 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:31.274061918 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 16:47:32.141752005 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:32.190381050 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 16:47:42.827264071 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:42.890696049 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 16:47:49.601633072 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:49.661398888 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 16:47:56.964221954 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 16:47:57.026830912 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 16:48:28.179665089 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 16:48:28.254879951 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 16:48:31.128184080 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 16:48:31.186876059 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 16:48:39.086479902 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 16:48:39.148816109 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 16:48:52.079786062 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 16:48:52.147031069 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 16:49:11.718720913 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 16:49:11.776118040 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 16:49:14.520978928 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 16:49:14.589231014 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 16:49:19.059950113 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 16:49:19.249295950 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 16:49:19.282136917 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 16:49:19.339981079 CEST	53	58530	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 16:49:19.059950113 CEST	192.168.2.5	8.8.8.8	0x2bab	Standard query (0)	smtp.kaeiser.com	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.282136917 CEST	192.168.2.5	8.8.8.8	0x85a3	Standard query (0)	smtp.kaeiser.com	A (IP address)	IN (0x0001)

DNS Answers

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 16:49:19.249295950 CEST	8.8.8.8	192.168.2.5	0x2bab	No error (0)	smtp.kaeiser.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 16:49:19.249295950 CEST	8.8.8.8	192.168.2.5	0x2bab	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.249295950 CEST	8.8.8.8	192.168.2.5	0x2bab	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.249295950 CEST	8.8.8.8	192.168.2.5	0x2bab	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.249295950 CEST	8.8.8.8	192.168.2.5	0x2bab	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.339981079 CEST	8.8.8.8	192.168.2.5	0x85a3	No error (0)	smtp.kaeiser.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 16:49:19.339981079 CEST	8.8.8.8	192.168.2.5	0x85a3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.339981079 CEST	8.8.8.8	192.168.2.5	0x85a3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.339981079 CEST	8.8.8.8	192.168.2.5	0x85a3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 16:49:19.339981079 CEST	8.8.8.8	192.168.2.5	0x85a3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

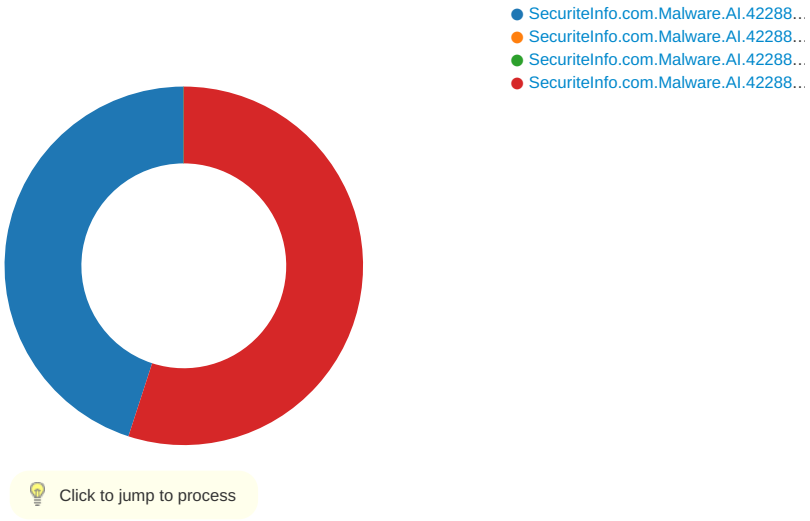
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 16:49:20.182816982 CEST	587	49733	208.91.199.224	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 12, 2021 16:49:20.183258057 CEST	49733	587	192.168.2.5	208.91.199.224	EHLO 124406
May 12, 2021 16:49:20.346596956 CEST	587	49733	208.91.199.224	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 12, 2021 16:49:20.349409103 CEST	49733	587	192.168.2.5	208.91.199.224	AUTH login c2VyZ2lvLmFycm95b0BrYWVpc2VyLmNvbQ==
May 12, 2021 16:49:20.513592005 CEST	587	49733	208.91.199.224	192.168.2.5	334 UGFzc3dvcmQ6
May 12, 2021 16:49:20.679681063 CEST	587	49733	208.91.199.224	192.168.2.5	235 2.7.0 Authentication successful
May 12, 2021 16:49:20.680565119 CEST	49733	587	192.168.2.5	208.91.199.224	MAIL FROM:<sergio.arroyo@kaeiser.com>
May 12, 2021 16:49:20.844995022 CEST	587	49733	208.91.199.224	192.168.2.5	250 2.1.0 Ok
May 12, 2021 16:49:20.845446110 CEST	49733	587	192.168.2.5	208.91.199.224	RCPT TO:<sergio.arroyo@kaeiser.com>
May 12, 2021 16:49:21.041570902 CEST	587	49733	208.91.199.224	192.168.2.5	250 2.1.5 Ok
May 12, 2021 16:49:21.042124033 CEST	49733	587	192.168.2.5	208.91.199.224	DATA
May 12, 2021 16:49:21.205835104 CEST	587	49733	208.91.199.224	192.168.2.5	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 16:49:21.211858034 CEST	49733	587	192.168.2.5	208.91.199.224	.
May 12, 2021 16:49:21.473221064 CEST	587	49733	208.91.199.224	192.168.2.5	250 2.0.0 Ok: queued as EE2481C20C4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Malware.AI.4228845530.13946.exe PID: 4012
Parent PID: 5796

General

Start time:	16:47:26
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe'
Imagebase:	0xa90000
File size:	934400 bytes
MD5 hash:	248B7D11FAB05DF72C28B150AF6F2DD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.258294495.0000000002F83000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.260145188.0000000003F85000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.260145188.0000000003F85000.00000004.00000001.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	6DCCCF06	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	6DCCCF06	unknown

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Malware.AI.4228845530.13946.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	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.Malware.AI.4228845530.13946.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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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,"Microsoft.VisualBasic, Ver	success or wait	1	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile

Analysis Process: SecuriteInfo.com.Malware.AI.4228845530.13946.exe PID: 488
Parent PID: 4012

Copyright Joe Security LLC 2021

General

Start time:	16:47:36
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
Imagebase:	0x240000
File size:	934400 bytes
MD5 hash:	248B7D11FAB05DF72C28B150AF6F2DD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Malware.AI.4228845530.13946.exe PID: 5596 Parent PID: 4012

General

Start time:	16:47:36
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
Imagebase:	0x310000
File size:	934400 bytes
MD5 hash:	248B7D11FAB05DF72C28B150AF6F2DD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Malware.AI.4228845530.13946.exe PID: 5756 Parent PID: 4012

General

Start time:	16:47:37
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Malware.AI.4228845530.13946.exe
Imagebase:	0xc80000
File size:	934400 bytes
MD5 hash:	248B7D11FAB05DF72C28B150AF6F2DD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.502628732.0000000003181000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.498013758.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.498013758.0000000000402000.00000040.00000001.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	6DCCCF06	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	6DCCCF06	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d54b7a8c-c8a0-4516-ac3e-c3849e56a052	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB11B4F	ReadFile

Disassembly

Code Analysis

Copyright Joe Security LLC 2021