ID: 385412
Sample Name:
SecuriteInfo.com.Trojan.PackedNET.645.19369.30388
Cookbook: default.jbs
Time: 13:09:06
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

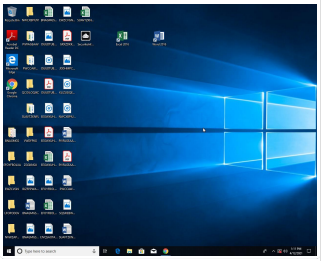
Analysis Report SecuriteInfo.com.Trojan.PackedNET.64…

Overview

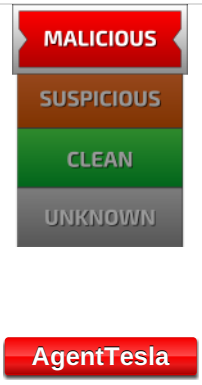
General Information

Sample Name:	SecuriteInfo.com.Trojan.PackedNET.645.19369.30388 (renamed file extension from 30388 to exe)
Analysis ID:	385412
MD5:	9a8808e03b68e5..
SHA1:	a9156e69f05b273.
SHA256:	1cdb81091d98d2..
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection

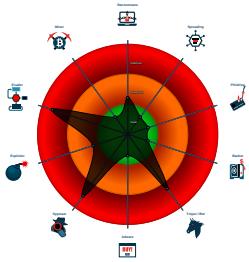


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.PackedNET.645.19369.exe (PID: 5668 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe' MD5: 9A8808E03B68E5C7A6B92389CF523684)
  - schtasks.exe (PID: 2392 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\YoNupIfnI' /XML 'C:\Users\user\AppData\Local\Temp\tmp4A35.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Trojan.PackedNET.645.19369.exe (PID: 2396 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe MD5: 9A8808E03B68E5C7A6B92389CF523684)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "wnahhas@alshareef-org.co@Sweden2020.,mail.privateemail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.479609173.0000000002DA5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.474023127.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.240720459.0000000002A31000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 6 entries				

Unpacked PEs

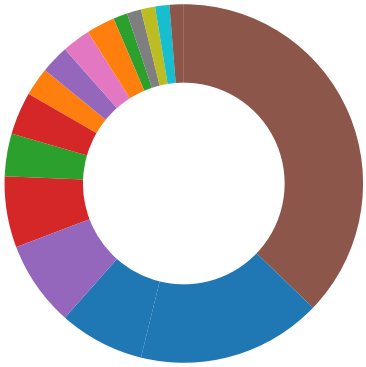
Source	Rule	Description	Author	Strings
3.2.SecuriteInfo.com.Trojan.PackedNET.645.19369.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.PackedNET.645.19369.exe.3cf7ef8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.PackedNET.645.19369.exe.3cf7ef8.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

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 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)

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:

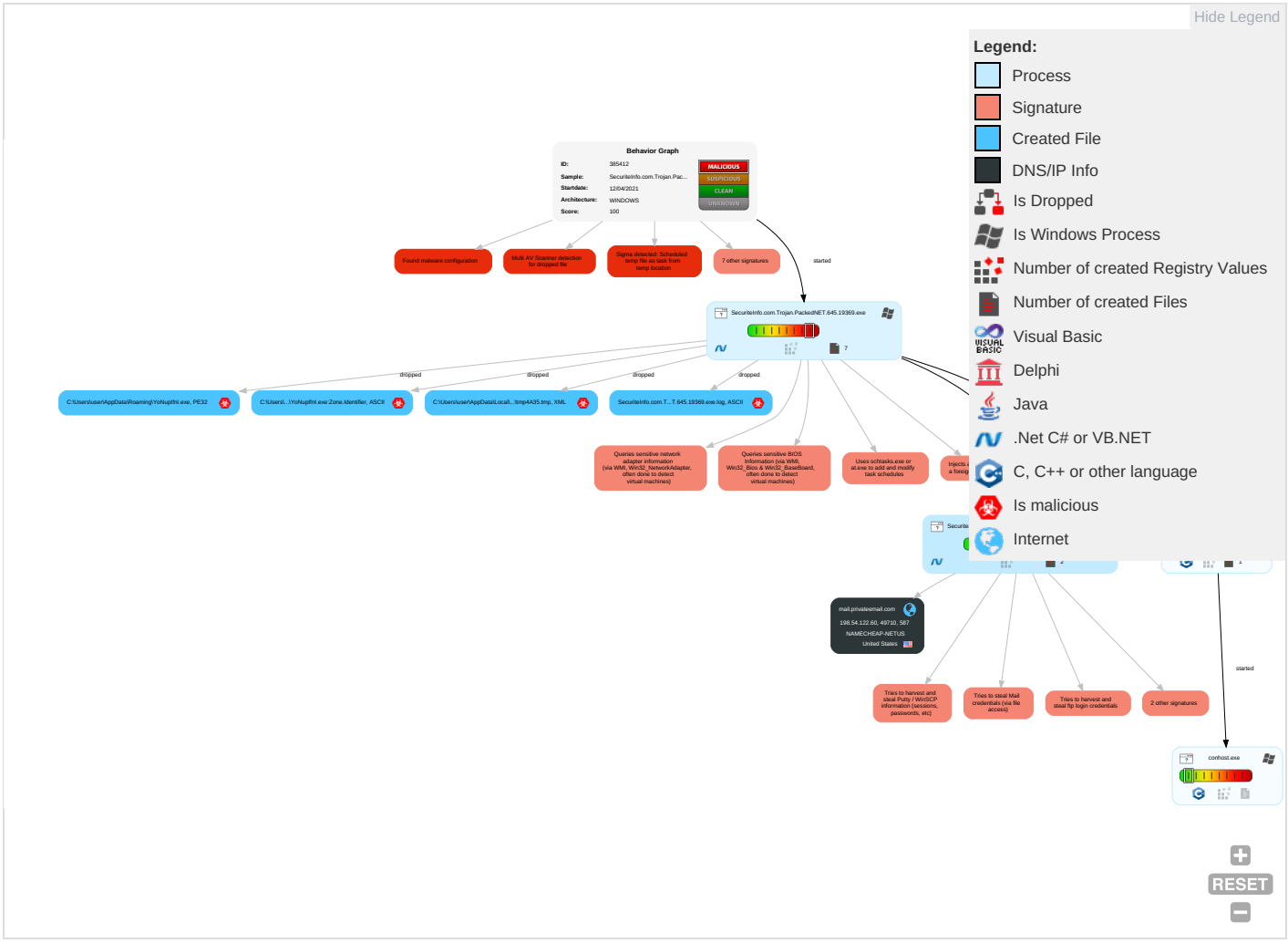
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
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	Account 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	File and Directory Discovery 1	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	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	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 Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System 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.645.19369.exe	33%	ReversingLabs	Win32.Trojan.Wacatac	
SecuriteInfo.com.Trojan.PackedNET.645.19369.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\YoNupIfnI.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\YoNupIfnI.exe	33%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.SecuriteInfo.com.Trojan.PackedNET.645.19369.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://NJDUeI.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comF7	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/chet	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/he	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://www.fontbureau.com=	0%	Avira URL Cloud	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://www.fontbureau.comsiva	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.sakkal.comP	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://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	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://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fontbureau.comG	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed-	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ild	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/q	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://NJDUeI.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high

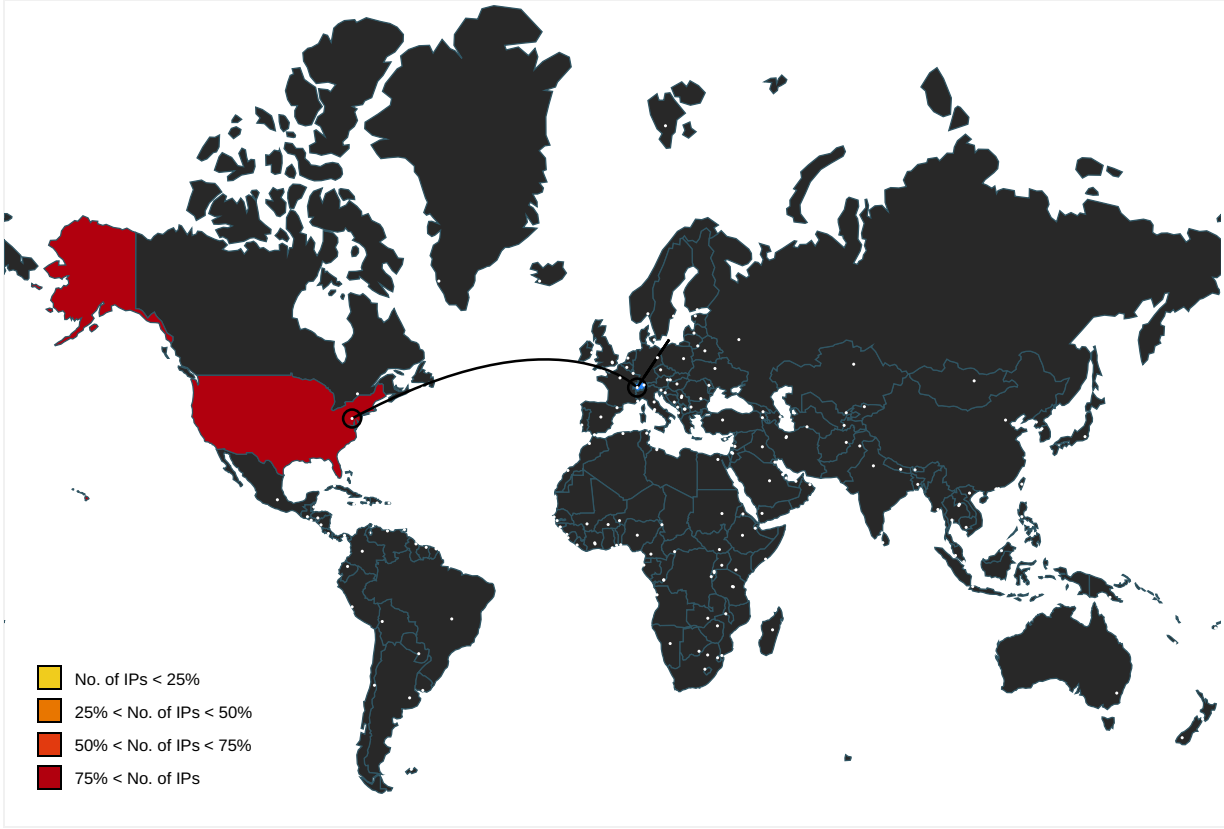
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.477604889.00000000011B2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.241052171.0000000002A7A000.00000004.00000001.sdmp	false		high
http://www.tiro.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.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.Trojan.PackedNET.645.19369.exe, 00000000.00000002.240720459.0000000002A31000.00000004.00000001.sdmp	false		high
http://www.fontbureau.coml1	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.237285257.0000000005AB0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.210156054.0000000005AB3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF7	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnn	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.212298152.0000000005ABD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.218123578.0000000005AC3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/chet	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/8	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/-	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215711492.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comd	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.210156054.0000000005AB3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.241052171.0000000002A7A000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.240360424.00000000029E1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215821511.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/he	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215821511.0000000005AB5000.00000004.00000001.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	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.244321688.0000000003B89000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.474023127.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com=	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.237285257.0000000005AB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.477604889.00000000011B2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comsiva	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.218123578.0000000005AC3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comP	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215711492.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/X	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215821511.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.477604889.00000000011B2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comc	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.210605693.0000000005ACB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comG	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comessed-	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/N	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ild	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215821511.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/q	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.privateemail.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.480002656.0000000002E10000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/x	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.212835401.0000000005AB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.212835401.0000000005AB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.216774100.0000000005AC9000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/p	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn2	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.212835401.0000000005AB8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215821511.0000000005AB5000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/-	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215821511.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comrsivc	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000002.248499293.0000000006CC2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/j	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://0SCo6pf5oOU.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000002.479609173.0000000002DA5000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000003.00000003.445621812.0000000000F74000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/c	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215537501.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/d	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.215821511.0000000005AB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.216478199.0000000005AEE000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comsief	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe, 00000000.00000003.217221192.0000000005AB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.122.60	mail.privateemail.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385412
Start date:	12.04.2021
Start time:	13:09:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.PackedNET.645.19369.30388 (renamed file extension from 30388 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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/4@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 27.3% • Quality standard deviation: 31.9%
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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209, 93.184.220.29, 205.185.216.42, 205.185.216.10, 104.43.139.144, 13.88.21.125, 168.61.161.212, 13.64.90.137, 184.30.24.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, cs9.wac.phicdn.net, fs.microsoft.com, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, ocsp.digicert.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus15.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385412/sample/SecuriteInfo.com.Trojan.PackedNET.645.19369.exe

Simulations

Behavior and APIs

Time	Type	Description
13:10:03	API Interceptor	700x Sleep call for process: SecuriteInfo.com.Trojan.PackedNET.645.19369.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	01_Enquiry Form.doc	Get hash	malicious	Browse	
	Quotation2001100200.PDF.exe	Get hash	malicious	Browse	
	Tepic.exe	Get hash	malicious	Browse	
	3.exe	Get hash	malicious	Browse	
	New#PO23000.PDF.exe	Get hash	malicious	Browse	
	l1l6llUtw7.exe	Get hash	malicious	Browse	
	dCallsd8lu.exe	Get hash	malicious	Browse	
	QzieSGrrlc.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6ptKQe0Bf8.exe	Get hash	malicious	Browse	
	P.O.exe	Get hash	malicious	Browse	
	POM-20120273.PDF.exe	Get hash	malicious	Browse	
	Purchase_order_pdf.exe	Get hash	malicious	Browse	
	purchase_order_pdf.exe	Get hash	malicious	Browse	
	Purchase_order_pdf.exe	Get hash	malicious	Browse	
	Order_BC012356PDF.exe	Get hash	malicious	Browse	
	PAYMENT ADVICE.pdf.exe	Get hash	malicious	Browse	
	RFQ 4917 21-006-AA.doc	Get hash	malicious	Browse	
	Pump_Motor-TENDER SPECIFICATION.doc	Get hash	malicious	Browse	
	Purchase Order_3006164.doc	Get hash	malicious	Browse	
	FORM E.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	01_Enquiry Form.doc	Get hash	malicious	Browse	• 198.54.122.60
	Quotation2001100200.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	Tepic.exe	Get hash	malicious	Browse	• 198.54.122.60
	3.exe	Get hash	malicious	Browse	• 198.54.122.60
	New#PO23000.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	l1l6llUtw7.exe	Get hash	malicious	Browse	• 198.54.122.60
	dCallsd8lu.exe	Get hash	malicious	Browse	• 198.54.122.60
	QzieSGrrlc.exe	Get hash	malicious	Browse	• 198.54.122.60
	6ptKQe0Bf8.exe	Get hash	malicious	Browse	• 198.54.122.60
	P.O.exe	Get hash	malicious	Browse	• 198.54.122.60
	POM-20120273.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase_order_pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	purchase_order_pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase_order_pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Order_BC012356PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	PAYMENT ADVICE.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ 4917 21-006-AA.doc	Get hash	malicious	Browse	• 198.54.122.60
	Pump_Motor-TENDER SPECIFICATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	Purchase Order_3006164.doc	Get hash	malicious	Browse	• 198.54.122.60
	FORM E.doc	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Bank Details.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	Import shipment.exe	Get hash	malicious	Browse	• 198.54.126.165
	01_Enquiry Form.doc	Get hash	malicious	Browse	• 198.54.122.60
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 198.54.126.105
	8Pd6TOKQOf.exe	Get hash	malicious	Browse	• 199.193.7.228
	Quotation2001100200.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	remittance info.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 162.0.229.227
	Swift002.exe	Get hash	malicious	Browse	• 198.54.117.211
	winlog.exe	Get hash	malicious	Browse	• 198.54.117.217
	2021-Quotation.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	36ne6xnkop.exe	Get hash	malicious	Browse	• 198.54.126.105
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 198.54.126.105
	Dridex.xls	Get hash	malicious	Browse	• 198.54.114.131
	Remittance Advice (1).xls	Get hash	malicious	Browse	• 198.54.114.220
	Remittance Advice (1).xls	Get hash	malicious	Browse	• 198.54.114.220
	Remittance Advice (1).xls	Get hash	malicious	Browse	• 198.54.114.220
	giATspz5dw.exe	Get hash	malicious	Browse	• 104.219.248.15
	Tepic.exe	Get hash	malicious	Browse	• 198.54.122.60
	3.exe	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\YoNupIfnI.exe	01_Enquiry Form.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.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\tmp4A35.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.187435806426066
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBrItn:cbh47TlNQ//rydbz9l3YODOLNdq3xu
MD5:	BFBA4EA1C4D901B4B93119378A4E936E
SHA1:	2A298DF813823CF1913D40191A81C8E7E10B2C6C
SHA-256:	50923D1670374A75F814026B607FFD8E1DA5EF0D92B63335691CD1AACCA9F21F
SHA-512:	54E73206FDDF6647D43E6E1F597477601EA9231A4FA926BD00D7EDD85BC6B1FFED2417376B83FD0D9A499E0FA32D29F70F9E6ACA960BE53091C7C1533F231DD
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>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\YoNupIfnI.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.702101602628262
Encrypted:	false
SSDEEP:	12288:jZOLC97rscaT4ytvT3aB1FK7CEfZgXRj9QAD1lCUUH0BgJxzKFMjvLe:jaksVMytjmFKWJjyAJUxU/UvLe
MD5:	9A8808E03B68E5C7A6B92389CF523684
SHA1:	A9156E69F05B27350444AA07228D4AA15799484C
SHA-256:	1CDB81091D98D217A4CDC8C570DF9178E797AF21A9D4B1BC39C49766322AE4BF
SHA-512:	E3262957BCB284C11E8B53E5D576591512782AE11F508A7B3ABA68DB3907FF9560206E07D55DF49A3A0D43631F83F65B62CF9ACA9DFE5BE50472D8FE8D04584E

C:\Users\user\AppData\Roaming\YoNupIfnI.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Joe Sandbox View:	• Filename: 01_Enquiry Form.doc, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z.s`.....P..J.....i... .....@.. .....@..... ..@.....ti..O..... ..... ..... ..H.....text....I... ...J..... ..`.rsrc.....L.....@..@.reloc..... .....@..B.....i.....H.....$}...v.....,...Hv.....0.....(....(.....(.....o!....*.....("......(#.....($.....(%.....(&....*N..(....o....('....*&.. ((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....,r. ..p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\YoNupIfnI.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.702101602628262
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe
File size:	905216
MD5:	9a8808e03b68e5c7a6b92389cf523684
SHA1:	a9156e69f05b27350444aa07228d4aa15799484c
SHA256:	1cdb81091d98d217a4cdc8c570df9178e797af21a9d4b1bc39c49766322ae4bf
SHA512:	e3262957bcb284c11e8b53e5d576591512782ae11f508a7b3aba68db3907ff9560206e07d55df49a3a0d43631f83f65b62cf9aca9dfe5be50472d8fe8d04584e
SSDEEP:	12288:jZOLC97rscaT4ytvT3aB1FK7CEfZgXRj9QAD1lCUUH0BgJxzKFMjvLe:jaksVMytjmFKWJjyAJUxU/UvLe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z.s`.....P..J.....i... .....@.. .....@.....@.....

File Icon

Icon Hash:	d28ab3b0e0ab96c4

Static PE Info

General	
Entrypoint:	0x4b69c6
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:	0x6073D57A [Mon Apr 12 05:07:06 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xb6974	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x2801c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	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	0xb49cc	0xb4a00	False	0.954884839965	data	7.95185598846	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x2801c	0x28200	False	0.347345940421	data	5.34681505935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8280	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc8aa8	0x94a8	data		
RT_ICON	0xd1f50	0x5488	data		
RT_ICON	0xd73d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xdb600	0x25a8	data		
RT_ICON	0xddba8	0x10a8	data		
RT_ICON	0xdec50	0x988	data		
RT_ICON	0xdf5d8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xdfa40	0x76	data		
RT_VERSION	0xdfab8	0x376	data		
RT_MANIFEST	0xdfe30	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

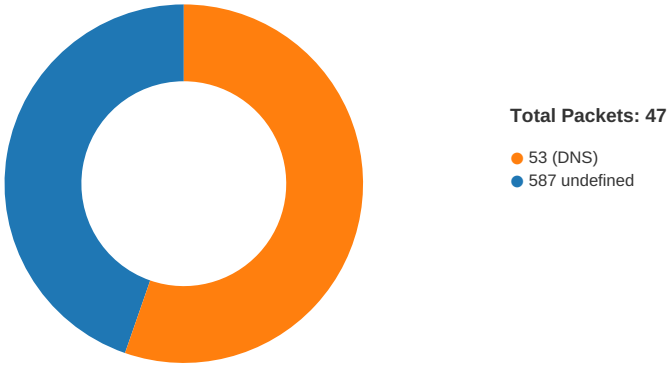
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2012
Assembly Version	8.1.1.15
InternalName	AssemblyName.exe
FileVersion	8.1.1.14
CompanyName	Landskip Yard Care
LegalTrademarks	A++
Comments	
ProductName	LevelActivator
ProductVersion	8.1.1.14
FileDescription	LevelActivator
OriginalFilename	AssemblyName.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:11:50.742096901 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:50.936301947 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:50.936518908 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:51.135938883 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.136396885 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:51.332415104 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.332446098 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.332948923 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:51.526618004 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.582125902 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:51.610776901 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:51.805519104 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.806893110 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.806910038 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.806927919 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.806946039 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:51.807065010 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:51.807109118 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:51.841373920 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:52.037518024 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.037543058 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.097805023 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:52.324698925 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:52.520371914 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.520828009 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.523878098 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:52.722922087 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.722948074 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.723623037 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:52.917310953 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.919341087 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:52.920392036 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:53.114203930 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.116560936 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.117043972 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:53.310775042 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.340661049 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.341113091 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:53.534807920 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.535516977 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.540888071 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:53.541090012 CEST	49710	587	192.168.2.3	198.54.122.60

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:11:53.541202068 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:53.541321993 CEST	49710	587	192.168.2.3	198.54.122.60
Apr 12, 2021 13:11:53.734632969 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.734662056 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.734821081 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.735452890 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.823827982 CEST	587	49710	198.54.122.60	192.168.2.3
Apr 12, 2021 13:11:53.879148960 CEST	49710	587	192.168.2.3	198.54.122.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:09:48.964338064 CEST	51904	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:49.023612022 CEST	53	51904	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:49.167671919 CEST	61328	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:49.216269016 CEST	53	61328	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:49.415568113 CEST	54130	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:49.466809034 CEST	53	54130	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:53.340708971 CEST	56961	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:53.402669907 CEST	53	56961	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:54.577980042 CEST	59353	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:54.629452944 CEST	53	59353	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:55.766333103 CEST	52238	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:55.814935923 CEST	53	52238	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:57.239907980 CEST	49873	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:57.290364981 CEST	53	49873	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:58.314894915 CEST	53196	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:09:58.371818066 CEST	53	53196	8.8.8.8	192.168.2.3
Apr 12, 2021 13:09:59.358244896 CEST	56777	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:00.370313883 CEST	56777	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:00.422017097 CEST	53	56777	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:01.323955059 CEST	58643	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:01.375555038 CEST	53	58643	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:02.585973978 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:02.637609959 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:03.666877985 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:03.721204042 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:04.818079948 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:04.869364023 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:05.722757101 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:05.771492004 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:06.696846962 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:06.745531082 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:07.795016050 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:07.846544027 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:09.025520086 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:09.088735104 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:10.127907038 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:10.178265095 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:11.705637932 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:11.762789965 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:14.528107882 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:14.579634905 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:15.478102922 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:15.526719093 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:18.285984993 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:18.335320950 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:23.788629055 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:23.850790024 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 13:10:49.670677900 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:10:49.719584942 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 13:11:50.586312056 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 13:11:50.638806105 CEST	53	60100	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 13:11:50.586312056 CEST	192.168.2.3	8.8.8.8	0x6a1e	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 13:11:50.638806105 CEST	8.8.8.8	192.168.2.3	0x6a1e	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

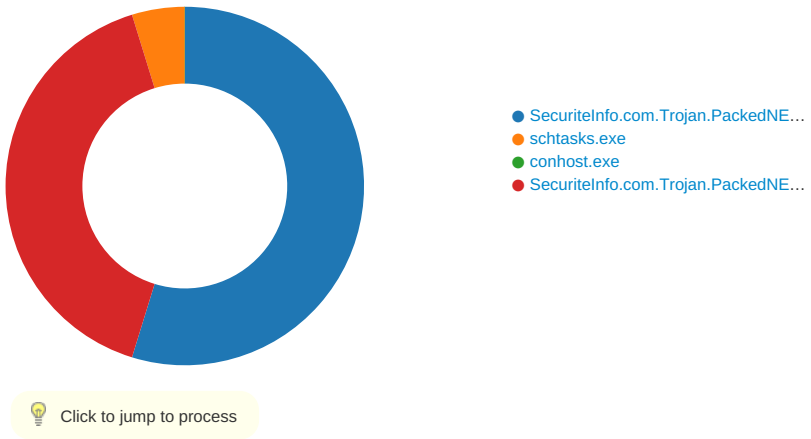
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 13:11:51.135938883 CEST	587	49710	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Apr 12, 2021 13:11:51.136396885 CEST	49710	587	192.168.2.3	198.54.122.60	EHLO 760639
Apr 12, 2021 13:11:51.332446098 CEST	587	49710	198.54.122.60	192.168.2.3	250-mta-14.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Apr 12, 2021 13:11:51.332948923 CEST	49710	587	192.168.2.3	198.54.122.60	STARTTLS
Apr 12, 2021 13:11:51.526618004 CEST	587	49710	198.54.122.60	192.168.2.3	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.PackedNET.645.19369.exe PID: 5668
Parent PID: 5692

General

Start time:	13:09:56
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe'
Imagebase:	0x6b0000
File size:	905216 bytes
MD5 hash:	9A8808E03B68E5C7A6B92389CF523684
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: 00000000.00000002.240720459.0000000002A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.244321688.0000000003B89000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming\YoNupIfnI.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	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\YoNupIfnI.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF4DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4A35.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF47038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4A35.tmp	success or wait	1	6CF46A95	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\YoNupIfnI.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 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 7a d5 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 4a 0b 00 00 84 02 00 00 00 00 00 c6 69 0b 00 00 20 00 00 00 80 0b 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 40 0e 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...z.s`.......... ....P..J...........i... ....@.. ....@ ....@................	success or wait	4	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\YoNupIfnI.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	6CF4DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4A35.tmp	unknown	1642	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 68 61 72 64 7a 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 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CF41B4F	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.645.19369.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, PublicKeyTok en=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: schtasks.exe PID: 2392 Parent PID: 5668

General

Start time:	13:10:09
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\YoNupIfnI' /XML 'C:\Users\user\AppData\Local\Temp\tmp4A35.tmp'
Imagebase:	0xec0000
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\tmp4A35.tmp	unknown	2	success or wait	1	ECAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4A35.tmp	unknown	1643	success or wait	1	ECABD9	ReadFile

Analysis Process: conhost.exe PID: 1832 Parent PID: 2392

General

Start time:	13:10:09
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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.645.19369.exe PID: 2396 Parent PID: 5668

General

Start time:	13:10:09
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.19369.exe
Imagebase:	0x950000
File size:	905216 bytes
MD5 hash:	9A8808E03B68E5C7A6B92389CF523684
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.479609173.0000000002DA5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.474023127.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.479122659.0000000002D41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.479367965.0000000002D79000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF41B4F	ReadFile

Disassembly

Code Analysis