ID: 413010
Sample Name:
SecuriteInfo.com.Trojan.Packed2.43091.16530.25305
Cookbook: default.jbs
Time: 06:04:14
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

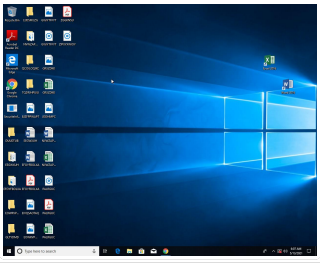
Analysis Report SecuriteInfo.com.Trojan.Packed2.43091…

Overview

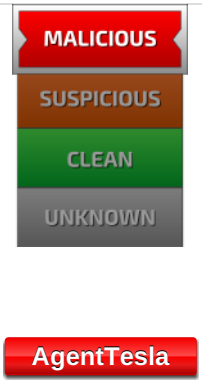
General Information

Sample Name:	SecuriteInfo.com.Trojan.Packed2.43091.16530.25305 (renamed file extension from 25305 to exe)
Analysis ID:	413010
MD5:	0b4cc13de8c54a…
SHA1:	4fb70edd4a74ea9…
SHA256:	579d75fb8f8f893…
Infos:	

Most interesting Screenshot:



Detection

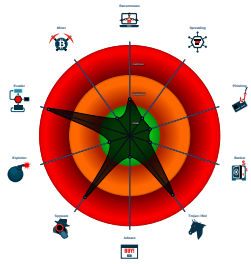


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.Packed2.43091.16530.exe (PID: 5360 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe' MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
  - SecuriteInfo.com.Trojan.Packed2.43091.16530.exe (PID: 6024 cmdline: {path} MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
- Nwefile.exe (PID: 6656 cmdline: 'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe' MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
  - Nwefile.exe (PID: 6728 cmdline: {path} MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
- Nwefile.exe (PID: 6764 cmdline: 'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe' MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sales@orienttech.com.qaOp{^fLb9gN[!mail.orienttech.com.qapdsctsops@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.262960133.0000000003D9C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.262960133.0000000003D9C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.502297847.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.502297847.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.509100287.00000000030F1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

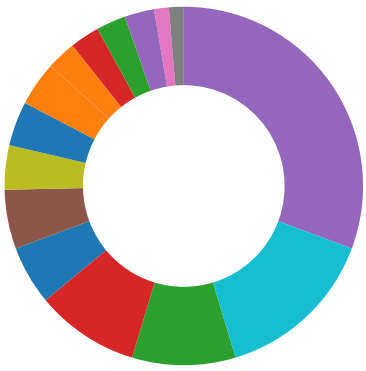
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.SecuriteInfo.com.Trojan.Packed2.43091.16530.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.SecuriteInfo.com.Trojan.Packed2.43091.16530.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
16.2.Nwefile.exe.45a6f20.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.Nwefile.exe.45a6f20.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.Packed2.43091.16530.exe.3e36f20.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected AgentTesla

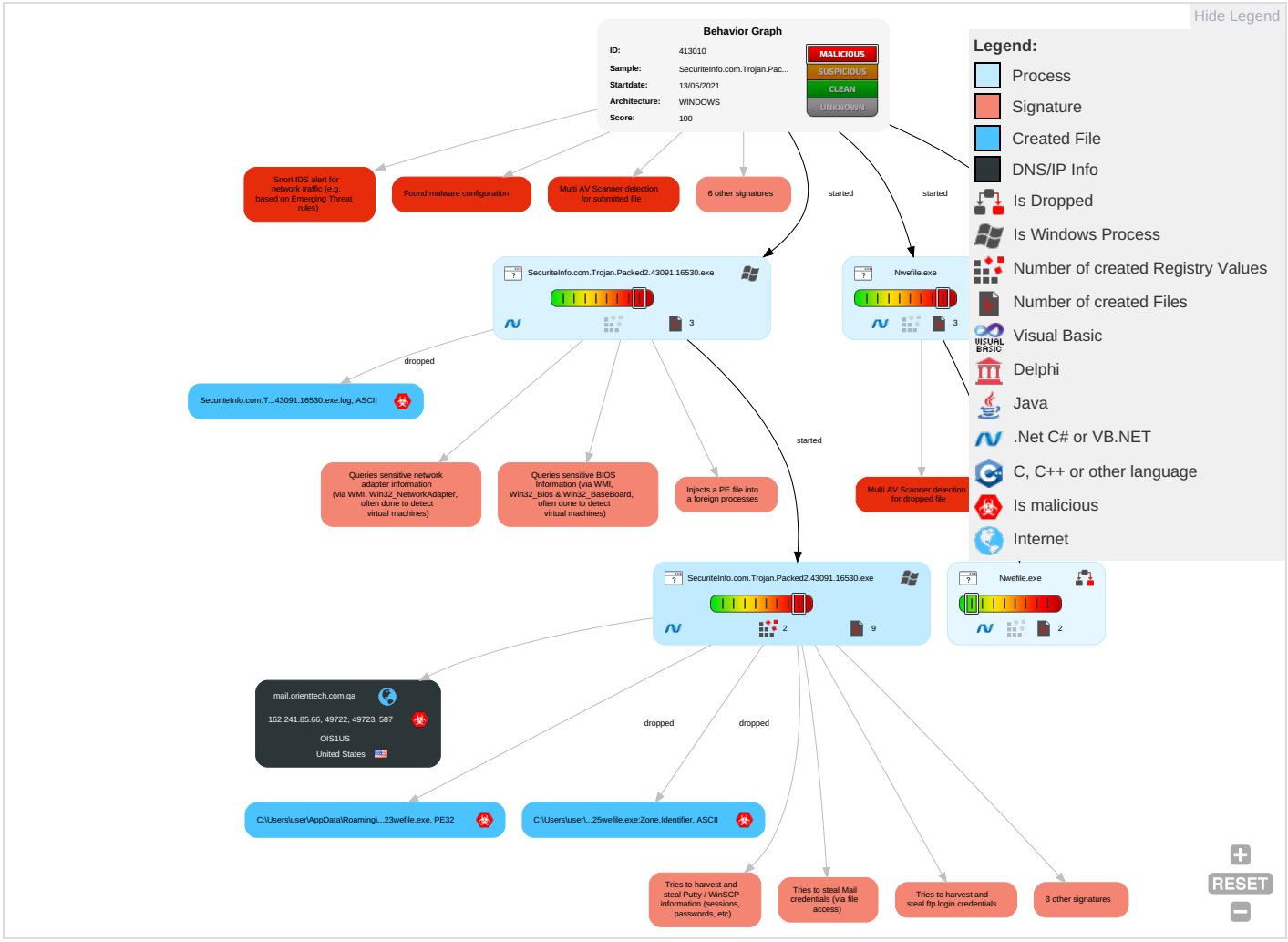
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Query Registry 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 2	Credentials in Registry 1	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applicatio Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Applicatio Layer Protocol 1

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

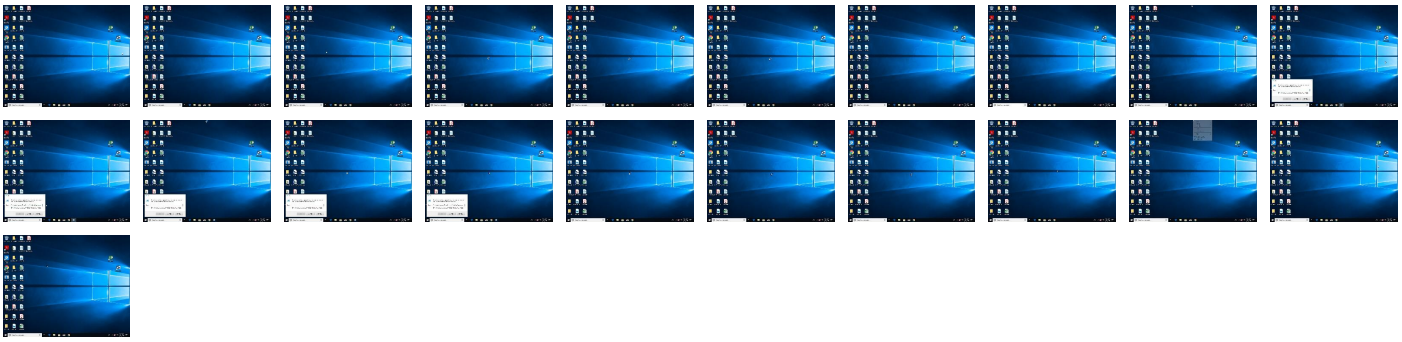
Behavior Graph



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.Packed2.43091.16530.exe	41%	Virustotal		Browse
SecuriteInfo.com.Trojan.Packed2.43091.16530.exe	35%	Metadefender		Browse
SecuriteInfo.com.Trojan.Packed2.43091.16530.exe	55%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	35%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	55%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.SecuriteInfo.com.Trojan.Packed2.43091.16530.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.2.Nwefile.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.orienttech.com.qa	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://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://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://mail.orienttech.com.qa	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://LROhh9NkeQD.net	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://yyfqMq.com	0%	Avira URL Cloud	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.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	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.orienttech.com.qa	162.241.85.66	true	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000003.000000002.509100287.00000000030F1000.00000004.00000001.sdmp, Nwefile.exe, 00000011.00000002.508052522.0000000002DD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	Nwefile.exe, 00000011.00000002.508052522.0000000002DD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.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.Packed2.43091.16530.exe, 00000003.000000002.509100287.00000000030F1000.00000004.00000001.sdmp, Nwefile.exe, 00000011.00000002.508052522.0000000002DD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.orienttech.com.qa	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000003.000000002.511083778.00000000033D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000003.000000002.509100287.00000000030F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://LROhh9NkeQD.net	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000003.000000002.509100287.00000000030F1000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000003.00000002.510923900.00000000033B8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://yyfqMq.com	Nwefile.exe, 00000011.00000002.508052522.0000000002DD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	Nwefile.exe, 00000011.00000002.508052522.0000000002DD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.270751560.0000000006CF2000.00000004.00000001.sdmp, Nwefile.exe, 00000010.00000002.363063227.00000000062B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000000.000000002.262960133.0000000003D9C000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.Packed2.43091.16530.exe, 00000003.00000002.502297847.000000000402000.00000040.00000001.sdmp, Nwefile.exe, 00000010.00000002.359038024.000000000450C000.00000004.00000001.sdmp, Nwefile.exe, 00000011.00000002.502572901.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.85.66	mail.orienttech.com.qa	United States		26337	OIS1US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413010
Start date:	13.05.2021
Start time:	06:04:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Packed2.43091.16530.25305 (renamed file extension from 25305 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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/5@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.3%) • Quality average: 40.1% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 20.82.210.154, 104.43.193.48, 40.88.32.150, 52.255.188.83, 92.122.145.220, 23.218.208.56, 20.50.102.62, 92.122.213.194, 92.122.213.247, 13.107.4.50, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, elasticShed.au.au-msedge.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, afdap.au.au-msedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, au.au-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • 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
06:05:16	API Interceptor	634x Sleep call for process: SecuriteInfo.com.Trojan.Packed2.43091.16530.exe modified
06:05:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Nwefile C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
06:05:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Nwefile C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
06:05:57	API Interceptor	388x Sleep call for process: Nwefile.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.85.66	99feb78a_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	Order QID R.exe	Get hash	malicious	Browse	
	scan doc_pdf.exe	Get hash	malicious	Browse	
	payment invoice.doc	Get hash	malicious	Browse	
	payment receipt.doc	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	wealthsecx.exe	Get hash	malicious	Browse	
	Bank receipt.doc	Get hash	malicious	Browse	
	07BhuWSD6z.exe	Get hash	malicious	Browse	
	LIST OF ITEMS.doc	Get hash	malicious	Browse	
	Drawings_pdf.exe	Get hash	malicious	Browse	
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.orienttech.com.qa	99feb78a_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 162.241.85.66
	Order QID R.exe	Get hash	malicious	Browse	• 162.241.85.66
	scan doc_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	payment invoice.doc	Get hash	malicious	Browse	• 162.241.85.66
	SecuriteInfo.com.Trojan.Siggen13.10233.30629.exe	Get hash	malicious	Browse	• 162.241.85.66
	payment receipt.doc	Get hash	malicious	Browse	• 162.241.85.66
	cLQd2QVOWu.exe	Get hash	malicious	Browse	• 162.241.85.66
	wealthsecx.exe	Get hash	malicious	Browse	• 162.241.85.66
	Bank receipt.doc	Get hash	malicious	Browse	• 162.241.85.66
	07BhuWSD6z.exe	Get hash	malicious	Browse	• 162.241.85.66
	LIST OF ITEMS.doc	Get hash	malicious	Browse	• 162.241.85.66
	Drawings_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	PO#BC210243_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	enquries.pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	SecuriteInfo.com.Artemis9DECF18E822A.1711.exe	Get hash	malicious	Browse	• 162.241.85.66
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 162.241.85.66

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OIS1US	99feb78a_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 162.241.85.66
	statistic-482095214.xls	Get hash	malicious	Browse	• 162.241.2.77
	statistic-482095214.xls	Get hash	malicious	Browse	• 162.241.2.77
	Order QID R.exe	Get hash	malicious	Browse	• 162.241.85.66
	slot Charges.exe	Get hash	malicious	Browse	• 162.241.85.231
	scan doc_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	generated order 257404.xlsm	Get hash	malicious	Browse	• 162.241.85.241
	9e7d034c_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	SecuriteInfo.com.VB.Trojan.Valyria.4579.10155.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	SecuriteInfo.com.VB.Trojan.Valyria.4579.10155.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	SecuriteInfo.com.VB.Trojan.Valyria.4579.18506.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	11710b54_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.147.20
	a37e9308_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.147.20
	8c2d96ab_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.85.231
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 192.185.14 7.148
	payment invoice.doc	Get hash	malicious	Browse	• 162.241.85.66
	Purchase Order_.exe	Get hash	malicious	Browse	• 162.241.85.194
	INVOICES..exe	Get hash	malicious	Browse	• 162.241.85.194
	INVOICE.pdf'.exe	Get hash	malicious	Browse	• 162.241.85.194
	svch.exe	Get hash	malicious	Browse	• 162.241.2.107

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Nwefile \Nwefile.exe	99feb78a_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nwefile.exe.log	
Process:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	758272
Entropy (8bit):	7.295996200857929
Encrypted:	false
SSDEEP:	12288:QoLLoS60/K7yh0AGWPlPjC6EPOyZoTRXq0R193e4hyOVj4:QoLAPWtP7uDK5R1p8Oq
MD5:	0B4CC13DE8C54ADD5149B56649B3F680
SHA1:	4FB70EDD4A74EA99D93225D8FC2901F699F1140F
SHA-256:	579D75FB8F8F893D2E1AE2845FC40E21EAB07AA6601B235E8C77F6E52956EF1A
SHA-512:	37A087FA83253AEE38EA440961A402F178EEB1209076E635B12DC829AAED691F81FFA637D148864AD8DACAD9BA66319A8605E71BBABC952F514F654B7FDE99C5
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 55%
Joe Sandbox View:	• Filename: 99feb78a_by_Libranalysis.xlsx, Detection: malicious, Browse
Reputation:	low

C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5L.....0..... .....@.. ..... .@.....O.....I..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...~.....v.....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..2.....($.....(%.....,...("......(&....('...(.....*>...(#...(.....*...0.....b`.+..*... ("... .....(...h..(!...h(....(Q...&*..0.....

C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.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**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\aoiyttac.0wl\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.295996200857929
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.Packed2.43091.16530.exe
File size:	758272
MD5:	0b4cc13de8c54add5149b56649b3f680
SHA1:	4fb70edd4a74ea99d93225d8fc2901f699f1140f
SHA256:	579d75fb8f8f893d2e1ae2845fc40e21eab07aa6601b235e8c77f6e52956ef1a
SHA512:	37a087fa83253aee38ea440961a402f178eeb1209076e65b12dc829aaed691f81ffa637d148864ad8dacad9ba66319a8605e71bbabc952f514f654b7fde99c5
SSDEEP:	12288:QoLLoS60/K7yh0AGWPlPjC6EPOyZoTRXq0R193e4hyOVj4:QoLAPWtP7uDK5R1p8Oq

General

File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L.... 5L...............0.................. ....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ba6da
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:	0xEA4C358C [Sun Jul 25 02:23:08 2094 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xba688	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xba66c	0x1c	.text
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	0xb86e0	0xb8800	False	0.725509188686	data	7.29768214208	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x5b4	0x600	False	0.422526041667	data	4.12543446876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	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_VERSION	0xbc090	0x324	data		
RT_MANIFEST	0xbc3c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

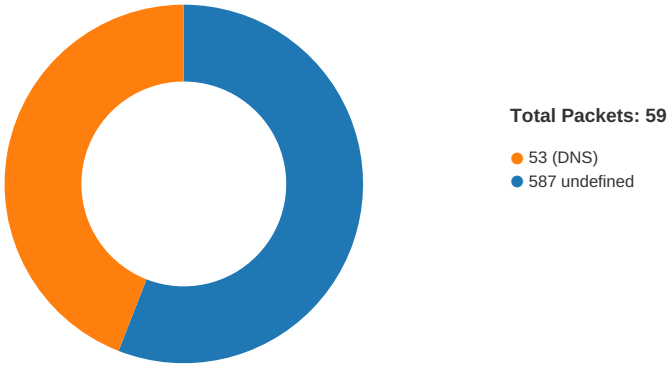
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	Ye8M26M.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Handle Leaker
ProductVersion	1.0.0.0
FileDescription	Handle Leaker
OriginalFilename	Ye8M26M.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/13/21-06:07:05.704494	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49722	587	192.168.2.5	162.241.85.66
05/13/21-06:07:08.757739	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49723	587	192.168.2.5	162.241.85.66

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:07:03.379409075 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:03.549276114 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:03.549410105 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:04.662606955 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:04.663248062 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:04.831068039 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:04.833679914 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.001773119 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.002398968 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.172358990 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.173135996 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.340769053 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.341134071 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.533045053 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.533449888 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.701210976 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.701334953 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.704493999 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.704684973 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.704766035 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.704848051 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:05.872199059 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.872572899 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:05.916074991 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:06.907932997 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:07.079555988 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:07.079672098 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:07.080610991 CEST	49722	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:07.177150965 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:07.248012066 CEST	587	49722	162.241.85.66	192.168.2.5
May 13, 2021 06:07:07.345539093 CEST	587	49723	162.241.85.66	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:07:07.345710039 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:07.716173887 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:07.716680050 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:07.884903908 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:07.885703087 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.054750919 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.055145979 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.224529028 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.225061893 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.393052101 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.393580914 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.585670948 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.585951090 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.754471064 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.754671097 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.757391930 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.757739067 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.757997990 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.758253098 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.758686066 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.759021044 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.759232044 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.759432077 CEST	49723	587	192.168.2.5	162.241.85.66
May 13, 2021 06:07:08.925841093 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.926426888 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.926902056 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.927658081 CEST	587	49723	162.241.85.66	192.168.2.5
May 13, 2021 06:07:08.978837967 CEST	49723	587	192.168.2.5	162.241.85.66

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:04:56.183542967 CEST	53784	53	192.168.2.5	8.8.8.8
May 13, 2021 06:04:56.250020981 CEST	53	53784	8.8.8.8	192.168.2.5
May 13, 2021 06:04:56.367510080 CEST	65307	53	192.168.2.5	8.8.8.8
May 13, 2021 06:04:56.416125059 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 06:04:56.995395899 CEST	64344	53	192.168.2.5	8.8.8.8
May 13, 2021 06:04:57.057681084 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 06:04:57.611598969 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 06:04:57.677109957 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 06:04:58.387732983 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 06:04:58.446877956 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 06:04:59.356535912 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 06:04:59.405196905 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 06:05:00.265825033 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:00.325500011 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 06:05:00.955691099 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:01.014228106 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 06:05:01.417916059 CEST	65447	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:01.477982998 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 06:05:02.653306007 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:02.704950094 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 06:05:04.149805069 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:04.199649096 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 06:05:05.482000113 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:05.531771898 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 06:05:07.323823929 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:07.375375032 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 06:05:08.308342934 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:08.359832048 CEST	53	63183	8.8.8.8	192.168.2.5
May 13, 2021 06:05:09.362171888 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:09.413798094 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 06:05:10.619376898 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:10.668090105 CEST	53	56969	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:05:23.189605951 CEST	55161	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:23.251789093 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 06:05:34.837431908 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:34.894886017 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 06:05:45.506675959 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:45.568212986 CEST	53	49992	8.8.8.8	192.168.2.5
May 13, 2021 06:05:51.192796946 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 06:05:51.244359970 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 06:06:12.538969040 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 06:06:12.596146107 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 06:06:16.096487045 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 06:06:16.153233051 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 06:06:45.270704031 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 06:06:45.336039066 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 06:06:56.683356047 CEST	54791	53	192.168.2.5	8.8.8.8
May 13, 2021 06:06:56.740473032 CEST	53	54791	8.8.8.8	192.168.2.5
May 13, 2021 06:07:03.123811960 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 06:07:03.347852945 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 06:07:07.116338015 CEST	50394	53	192.168.2.5	8.8.8.8
May 13, 2021 06:07:07.174647093 CEST	53	50394	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2021 06:07:03.123811960 CEST	192.168.2.5	8.8.8.8	0x90ad	Standard query (0)	mail.orienttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 06:07:07.116338015 CEST	192.168.2.5	8.8.8.8	0xfcb0	Standard query (0)	mail.orienttech.com.qa	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 06:07:03.347852945 CEST	8.8.8.8	192.168.2.5	0x90ad	No error (0)	mail.orienttech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 06:07:07.174647093 CEST	8.8.8.8	192.168.2.5	0xfcb0	No error (0)	mail.orienttech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)

SMTP Packets

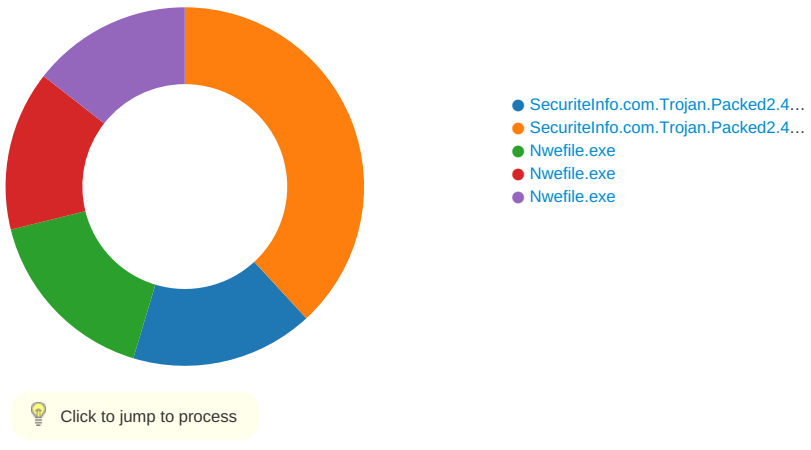
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2021 06:07:04.662606955 CEST	587	49722	162.241.85.66	192.168.2.5	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 04:07:04 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 06:07:04.663248062 CEST	49722	587	192.168.2.5	162.241.85.66	EHLO 841618
May 13, 2021 06:07:04.831068039 CEST	587	49722	162.241.85.66	192.168.2.5	250-sh002.bigrock.com Hello 841618 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 06:07:04.833679914 CEST	49722	587	192.168.2.5	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 06:07:05.001773119 CEST	587	49722	162.241.85.66	192.168.2.5	334 UGFzc3dvcmQ6
May 13, 2021 06:07:05.172358990 CEST	587	49722	162.241.85.66	192.168.2.5	235 Authentication succeeded
May 13, 2021 06:07:05.173135996 CEST	49722	587	192.168.2.5	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 06:07:05.340769053 CEST	587	49722	162.241.85.66	192.168.2.5	250 OK
May 13, 2021 06:07:05.341134071 CEST	49722	587	192.168.2.5	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 06:07:05.533045053 CEST	587	49722	162.241.85.66	192.168.2.5	250 Accepted
May 13, 2021 06:07:05.533449888 CEST	49722	587	192.168.2.5	162.241.85.66	DATA
May 13, 2021 06:07:05.701334953 CEST	587	49722	162.241.85.66	192.168.2.5	354 Enter message, ending with "." on a line by itself
May 13, 2021 06:07:05.704848051 CEST	49722	587	192.168.2.5	162.241.85.66	.
May 13, 2021 06:07:05.872572899 CEST	587	49722	162.241.85.66	192.168.2.5	250 OK id=1lh2cr-001fl4-KA
May 13, 2021 06:07:06.907932997 CEST	49722	587	192.168.2.5	162.241.85.66	QUIT
May 13, 2021 06:07:07.079555988 CEST	587	49722	162.241.85.66	192.168.2.5	221 sh002.bigrock.com closing connection

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2021 06:07:07.716173887 CEST	587	49723	162.241.85.66	192.168.2.5	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 04:07:07 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 06:07:07.716680050 CEST	49723	587	192.168.2.5	162.241.85.66	EHLO 841618
May 13, 2021 06:07:07.884903908 CEST	587	49723	162.241.85.66	192.168.2.5	250-sh002.bigrock.com Hello 841618 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 06:07:07.885703087 CEST	49723	587	192.168.2.5	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 06:07:08.054750919 CEST	587	49723	162.241.85.66	192.168.2.5	334 UGFzc3dvcmQ6
May 13, 2021 06:07:08.224529028 CEST	587	49723	162.241.85.66	192.168.2.5	235 Authentication succeeded
May 13, 2021 06:07:08.225061893 CEST	49723	587	192.168.2.5	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 06:07:08.393052101 CEST	587	49723	162.241.85.66	192.168.2.5	250 OK
May 13, 2021 06:07:08.393580914 CEST	49723	587	192.168.2.5	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 06:07:08.585670948 CEST	587	49723	162.241.85.66	192.168.2.5	250 Accepted
May 13, 2021 06:07:08.585951090 CEST	49723	587	192.168.2.5	162.241.85.66	DATA
May 13, 2021 06:07:08.754671097 CEST	587	49723	162.241.85.66	192.168.2.5	354 Enter message, ending with "." on a line by itself
May 13, 2021 06:07:08.759432077 CEST	49723	587	192.168.2.5	162.241.85.66	.
May 13, 2021 06:07:08.927658081 CEST	587	49723	162.241.85.66	192.168.2.5	250 OK id=1lh2cu-001fLa-Ls

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Packed2.43091.16530.exe PID: 5360
Parent PID: 5640

General

Start time:	06:05:06

Start date:	13/05/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe'
Imagebase:	0x7c0000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.262960133.0000000003D9C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.262960133.0000000003D9C000.00000004.00000001.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	6DAECF06	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	6DAECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDFC78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DDFC907	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile

Analysis Process: SecuriteInfo.com.Trojan.Packed2.43091.16530.exe PID: 6024
Parent PID: 5360

General

Start time:	06:05:17
Start date:	13/05/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43091.16530.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc80000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680

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: 00000003.00000002.502297847.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.502297847.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.509100287.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.509100287.00000000030F1000.00000004.00000001.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	6DAECF06	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	6DAECF06	unknown
C:\Users\user\AppData\Roaming\Nwefile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C93BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.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	6C93DD66	CopyFileW
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C93DD66	CopyFileW
C:\Users\user\AppData\Roaming\aoiyttac.0wl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C93BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\aoiyttac.0wl\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	6C93BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\aoiyttac.0wl\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	6C93BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\aoiyttac.0wl\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C93DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe:Zone.Identifier	success or wait	1	628BA1A	DeleteFileW
C:\Users\user\AppData\Roaming\aoiyttac.0wl\Chrome\Default\Cookies	success or wait	1	6C936A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.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 8c 35 4c ea 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 88 0b 00 00 08 00 00 00 00 00 00 da a6 0b 00 00 20 00 00 00 c0 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 00 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....5L........... ....0.................. ....@.. ....@................	success or wait	3	6C93DD66	CopyFileW
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.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	6C93DD66	CopyFileW
C:\Users\user\AppData\Roaming\aoiyttac.0wl\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 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 00 00 00 00 00 00 00 00 00 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	6C93DD66	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C931B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C931B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\1ec4f6a0-a557-4a8f-ae51-eec3dfe40c6b	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C931B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C931B4F	ReadFile
C:\Users\user\AppData\Roaming\aoiyttac.0wl\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C931B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Nwefile	unicode	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	success or wait	1	6C93646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	Nwefile	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C93DE2E	RegSetValueExW

Analysis Process: Nwefile.exe PID: 6656 Parent PID: 3472

General

Start time:	06:05:52
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe'
Imagebase:	0xe90000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
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: 00000010.00000002.359038024.000000000450C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.359038024.000000000450C000.00000004.00000001.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 35%, Metadefender, Browse • Detection: 55%, ReversingLabs
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	6DAECF06	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	6DAECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nwefile.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDFC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nwefile.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DDFC907	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile

Analysis Process: Nwefile.exe PID: 6728 Parent PID: 6656

General

Start time:	06:05:59
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x930000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
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: 00000011.00000002.508052522.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.508052522.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.502572901.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000002.502572901.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAECF06	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	6DAECF06	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile

Analysis Process: Nwefile.exe PID: 6764 Parent PID: 3472

General

Start time:	06:06:01
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe'
Imagebase:	0xf00000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6DAECF06	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	6DAECF06	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile

Disassembly

Code Analysis