ID: 385400
Sample Name:
SecuriteInfo.com.Trojan.PackedNET.645.23105.6482
Cookbook: default.jbs
Time: 12:58:52
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

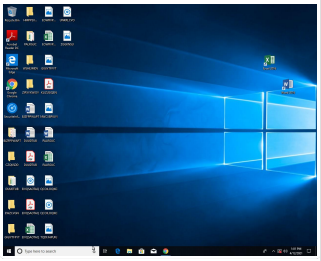
Analysis Report SecuriteInfo.com.Trojan.PackedNET.64…

Overview

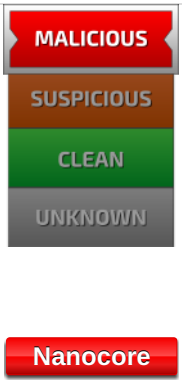
General Information

Sample Name:	SecuriteInfo.com.Trojan.PackedNET.645.23105.6482 (renamed file extension from 6482 to exe)
Analysis ID:	385400
MD5:	6a647fd057fd6a0..
SHA1:	0876b0bd85b3fea.
SHA256:	74e0f799a11a134.
Tags:	NanoCore
Infos:	

Most interesting Screenshot:



Detection



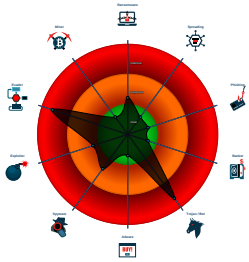
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.PackedNET.645.23105.exe (PID: 6484 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe' MD5: 6A647FD057FD6A0B85C644D928125EB4)
  - schtasks.exe (PID: 6704 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\blFUun' /XML 'C:\Users\user\AppData\Local\Temp\tmpF1BB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6840 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- dhcpmon.exe (PID: 6316 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f57d5a77-8670-45ef-b736-5f3a07b6",
  "Group": "Addora",
  "Domain1": "79.134.225.30",
  "Domain2": "nassiru1155.ddns.net",
  "Port": 1144,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.508372796.0000000004FD0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000006.00000002.508372796.0000000004FD0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000006.00000002.500192015.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000006.00000002.500192015.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000006.00000002.500192015.0000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q

Click to see the 16 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.RegSvcs.exe.4fd0000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
6.2.RegSvcs.exe.4fd0000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
6.2.RegSvcs.exe.3c39606.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d0af:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d0dc:$x2: IClientNetworkHost
6.2.RegSvcs.exe.3c39606.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d0af:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e18a:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d0c9:$s5: IClientLoggingHost
6.2.RegSvcs.exe.3c39606.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 34 entries				

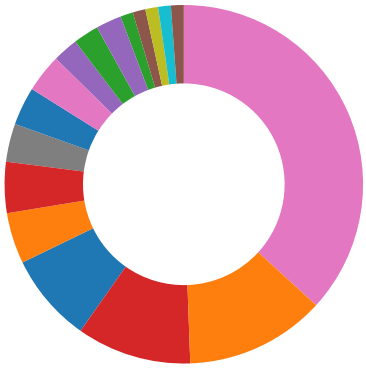
Sigma Overview

System Summary:

Sigma detected: NanoCore

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
- E-Banking Fraud
- 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

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

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

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

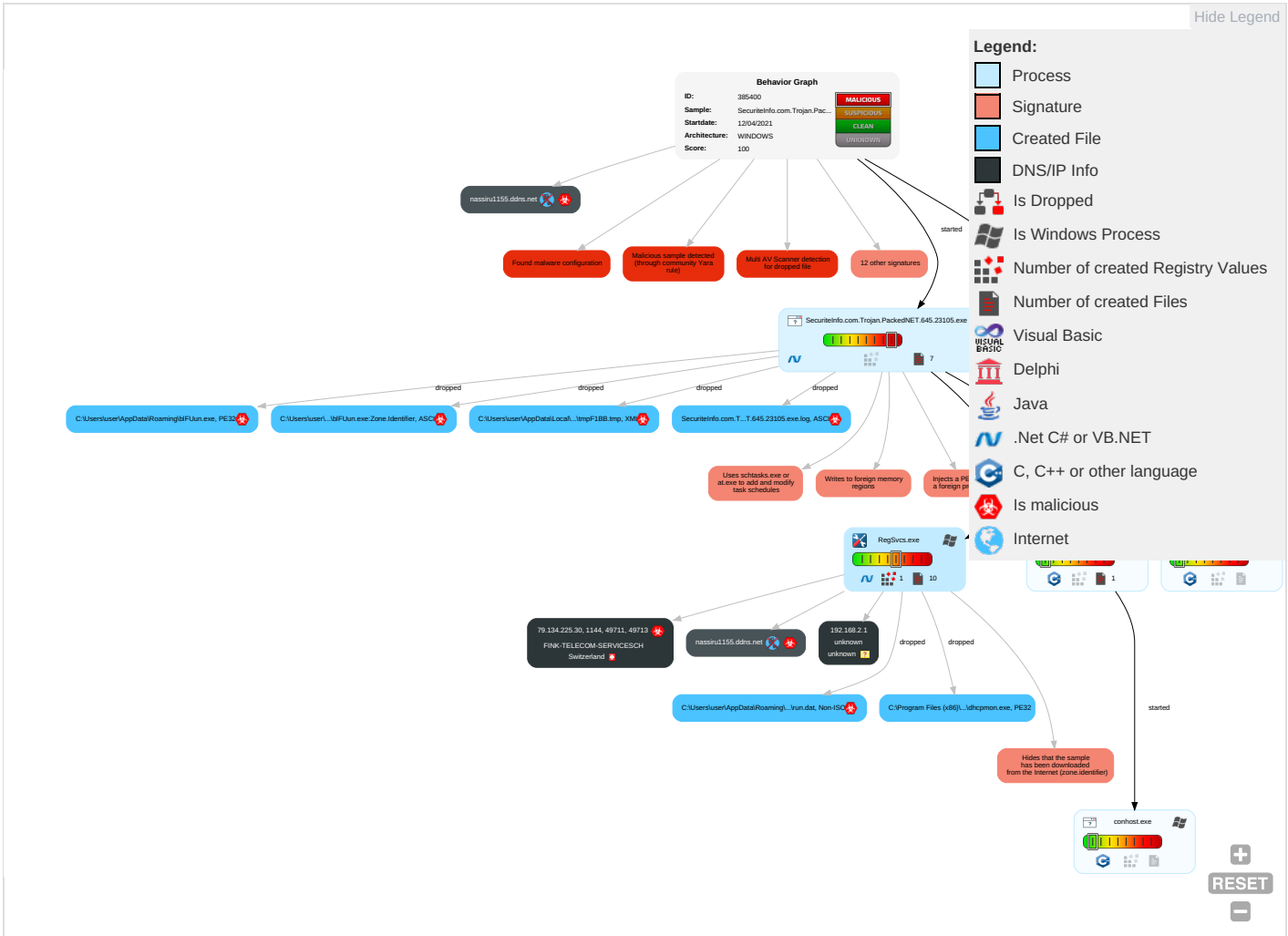
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

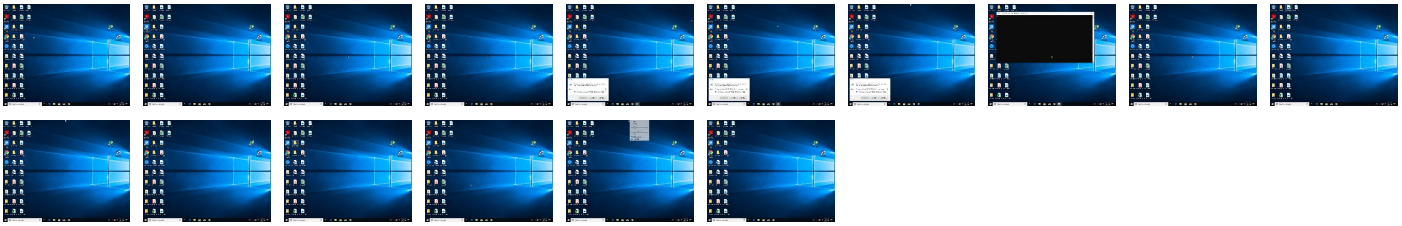
Behavior Graph



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.645.23105.exe	23%	Virustotal		Browse
SecuriteInfo.com.Trojan.PackedNET.645.23105.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SecuriteInfo.com.Trojan.PackedNET.645.23105.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\blFUun.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\blFUun.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.RegSvcs.exe.5420000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
nassiru1155.ddns.net	0%	Avira URL Cloud	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.fonts.comc	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://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	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://www.jiyu-kobo.co.jp/jp/3	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://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.tiro.comtn	0%	Avira URL Cloud	safe	
79.134.225.30	0%	Avira URL Cloud	safe	
http://www.fontbureau.comoW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Verd	0%	Avira URL Cloud	safe	
http://www.fontbureau.comionb	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.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	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	

Source	Detection	Scanner	Label	Link
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://www.sandoll.co.krR	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	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.jiyu-kobo.co.jp/ana	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	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.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.founder.com.cn/cnZ	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.jiyu-kobo.co.jp/rporW	0%	Avira URL Cloud	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://www.founder.com.cn/cn/0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnb	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nassiru1155.ddns.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nassiru1155.ddns.net	true	• Avira URL Cloud: safe	unknown
79.134.225.30	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

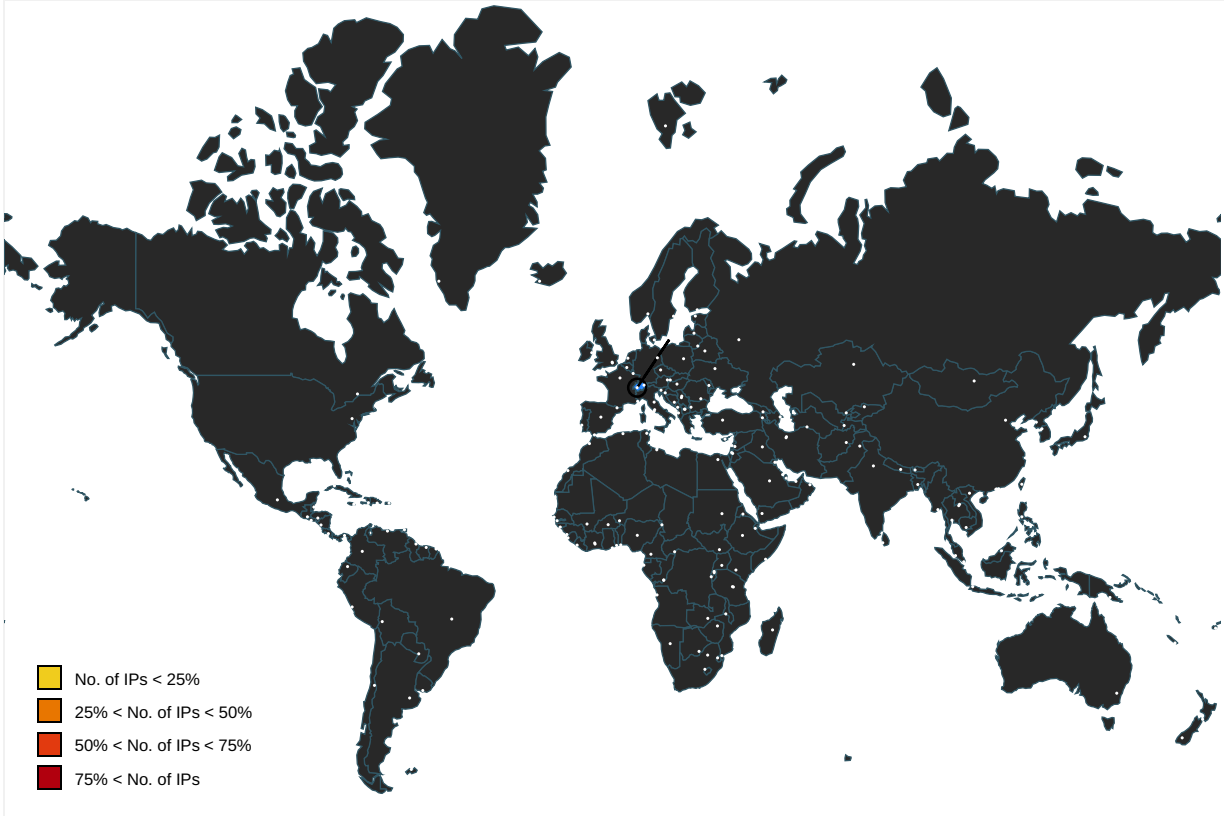
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.fonts.comc	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.233596538.0000000004DAB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.tiro.comn	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.233999912.0000000004DAB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.239806391.0000000004D99000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/3	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.237664305.0000000004D94000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.237664305.0000000004D94000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comtn	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.233961727.0000000004DAB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comoW	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.259368413.0000000004D90000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Verd	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.237664305.0000000004D94000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.261175350.0000000002AB1000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comionb	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.259368413.0000000004D90000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.233471489.0000000004DAE000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/y	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.237664305.0000000004D94000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.233961727.0000000004DAB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.235939955.0000000004D94000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krR	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.235097526.0000000004D96000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/p	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.237664305.0000000004D94000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.237664305.0000000004D94000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ana	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.237664305.0000000004D94000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.233596538.0000000004DAB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000002.270787684.0000000005FA2000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, 00000000.00000003.233654714.0000000004DAE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000003.235097526.0000000004D96 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnZ	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000003.235914807.0000000004DCD 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000002.270787684.0000000005FA2 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/rporW	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000003.237664305.0000000004D94 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000002.270787684.0000000005FA2 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000002.270787684.0000000005FA2 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/0	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000003.236190525.0000000004D94 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnb	SecuriteInfo.com.Trojan.Packed NET.645.23105.exe, 00000000.00 000003.235914807.0000000004DCD 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.30	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385400
Start date:	12.04.2021
Start time:	12:58:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.PackedNET.645.23105.6482 (renamed file extension from 6482 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:	29
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.evad.winEXE@8/8@36/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.9% (good quality ratio 1.2%) • Quality average: 38.5% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 93.184.220.29, 168.61.161.212, 20.82.210.154, 52.147.198.201, 92.122.145.220, 184.30.24.56, 20.50.102.62, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:59:53	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.PackedNET.645.23105.exe modified
13:00:00	API Interceptor	929x Sleep call for process: RegSvcs.exe modified
13:00:02	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.30	PR0078966.xlsx	Get hash	malicious	Browse	
	JQEl8bosea.exe	Get hash	malicious	Browse	
	YfceI5MZX4.exe	Get hash	malicious	Browse	
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	
	TSskTqG9V9.exe	Get hash	malicious	Browse	
	Files Specification.xlsx	Get hash	malicious	Browse	
	J62DQ7fO0b.exe	Get hash	malicious	Browse	
	oE6O5K1emC.exe	Get hash	malicious	Browse	
	AIC7VMxudf.exe	Get hash	malicious	Browse	
	Payment Confirmation.exe	Get hash	malicious	Browse	
	JOIN.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Itinerary.pdf.exe	Get hash	malicious	Browse	
	vVH0wIFYFd.exe	Get hash	malicious	Browse	
	GWee9QSphp.exe	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	
	Import and Export Regulation.xlsx	Get hash	malicious	Browse	
	BBdzKOGQ36.exe	Get hash	malicious	Browse	
	BL.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	PR0078966.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 79.134.225.21
	JQEl8bosea.exe	Get hash	malicious	Browse	• 79.134.225.30
	YfceI5MZX4.exe	Get hash	malicious	Browse	• 79.134.225.30
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	OjAJYVQ7iK.exe	Get hash	malicious	Browse	• 79.134.225.112
	TSskTqG9V9.exe	Get hash	malicious	Browse	• 79.134.225.30
	Files Specification.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	J62DQ7fO0b.exe	Get hash	malicious	Browse	• 79.134.225.30
	oE6O5K1emC.exe	Get hash	malicious	Browse	• 79.134.225.30
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	• 79.134.225.40
	EASTERS.exe	Get hash	malicious	Browse	• 79.134.225.118
	LIST OF POEA DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 79.134.225.9
	AWB.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	AIC7VMxudf.exe	Get hash	malicious	Browse	• 79.134.225.30
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 79.134.225.21
	PO50164.exe	Get hash	malicious	Browse	• 79.134.225.79
	Fast color scan to a PDFfile_1_20210331084231346.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	n7dlHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JQEl8bosea.exe	Get hash	malicious	Browse	
	YfceI5MZX4.exe	Get hash	malicious	Browse	
	TSskTqG9V9.exe	Get hash	malicious	Browse	
	oE6O5K1emC.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	wDIaJji4Vv.exe	Get hash	malicious	Browse	
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	
	Bilansno placanje.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.9647.20479.exe	Get hash	malicious	Browse	
	wnIPBdB5OF.exe	Get hash	malicious	Browse	
	Delivery Form C.exe	Get hash	malicious	Browse	
	h6uc8EaDQX.exe	Get hash	malicious	Browse	
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	
	sfTZCyMKuC.exe	Get hash	malicious	Browse	
	y9Rtu1cnBk.exe	Get hash	malicious	Browse	
	lxli7b5j6A.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nq0aCrCXyE.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: JQEl8bosea.exe, Detection: malicious, Browse • Filename: YfceI5MZX4.exe, Detection: malicious, Browse • Filename: TSskTqG9V9.exe, Detection: malicious, Browse • Filename: oE6O5K1emC.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: wDlaJji4Vv.exe, Detection: malicious, Browse • Filename: cJtVGjtNGZ.exe, Detection: malicious, Browse • Filename: Bilansno placanje.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Inject4.9647.20479.exe, Detection: malicious, Browse • Filename: wnIPBdB5OF.exe, Detection: malicious, Browse • Filename: Delivery Form C.exe, Detection: malicious, Browse • Filename: h6uc8EaDQX.exe, Detection: malicious, Browse • Filename: 3aDHivUqWtumbXb.exe, Detection: malicious, Browse • Filename: fMy120EQiT6NaRd.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.394792.29952.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.578.18498.exe, Detection: malicious, Browse • Filename: sfTZCyMKuC.exe, Detection: malicious, Browse • Filename: y9Rtu1cnBk.exe, Detection: malicious, Browse • Filename: Ixli7b5j6A.exe, Detection: malicious, Browse • Filename: nq0aCrCXyE.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k.. .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmpF1BB.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.164885803712183
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBhtn:cbhC7ZlNQF/rydbz9l3YODOLNdq3F
MD5:	C28E68C75ABD53356A5DF3074B107595
SHA1:	1EA9E5631C0A3219F6F9D1CDB2CCCD244203C17A
SHA-256:	1A3A54795AC2D429ACD796D1F6BC0D4BEA023AD797B6477E509503A1A78649DF
SHA-512:	49036930F99E31387C717F7C0CDE25F1D1FB1341C6281ED2DDD7C32BDE701029C339620AF7D14E78D5A79773574C837C6EC35B96A11D09512B7B49DC2D48156
Malicious:	**true**
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>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:V4:i
MD5:	220D3CA34B43CB89B617F08FF01E8030
SHA1:	4F809C4164A30EBE97459A81640B23E3C489FFA6
SHA-256:	86A4A49BF7D25857DD26986AC56372DEE58EC1D35D845408B22D63EB1A97B260
SHA-512:	07ECFF530F35AE5FADE3E1C099E038B0F95AF5E993F28EFA261B97EEA9123738CC818D323EF5B5BE294AAA3EA43BA69E24F92DCB8C7C31DCC06E6B0154F309 65
Malicious:	**true**
Preview:	[j.....H

C:\Users\user\AppData\Roaming\blFUun.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	792064
Entropy (8bit):	7.348021891570888
Encrypted:	false
SSDEEP:	12288:I4enekLI7hRNLPXlf/BfykeiLmtlzwrbsybFVxXo7Ko7ICfLcA:QFNLPXLxjLm7KoOVxXBjCfLcA
MD5:	6A647FD057FD6A0B85C644D928125EB4
SHA1:	0876B0BD85B3FEA743370B8A7793102DD9328BBB
SHA-256:	74E0F799A11A134C003BDFC626D453E74C92903D0640C8E1C801A78FE715A095
SHA-512:	0800B5ED2A4A608EE58D8679439E62533F9316B9F908D34F48C24A8BB7E106664BCA89E32B2A0C4532B4C736977FA83D03D4EDA980D05C89A35426EC740F7DA
Malicious:	**true**

C:\Users\user\AppData\Roaming\blFUun.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....I.....j.... .....@.. ..... ..@.....O.....4i.....` ....H.....text..... ....`.rsrc...4i.....j.....@..@.reloc.....` .....@..B.....L.....H.....x.....0.....(#...($.....(.....o%...*.....(&.....('.....((.....().....(*....*N..(....o....(+....*&.. (....*.s-.....s.....s/.....s0.....s1.....*....0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0..<.....~.....(7.....!r. ..p.....(8...o9...s:.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\blFUun.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.23105.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

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071E E
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [optio ns] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target app lication, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /rec onfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /no logo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	7.348021891570888
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.645.23105.exe
File size:	792064
MD5:	6a647fd057fd6a0b85c644d928125eb4
SHA1:	0876b0bd85b3fea743370b8a7793102dd9328bbb
SHA256:	74e0f799a11a134c003bdfc626d453e74c92903d0640c8e 1c801a78fe715a095

General

SHA512:	0800b5ed2a4a608ee58d8679439e62533f9316b9f908d3 f48c24a8bb7e106664bca89e32b2a0c4532b4c736977fa8 3d03d4eda980d05c89a35426ec740f7dac
SSDEEP:	12288:l4enekLl7hRNLPXlf/BfykeiLmtlzwrbsybFVxXo7K o7ICfLcA:QFNLPXLxjLm7KoOVxXBjCfLcA
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... s`.....P.....l.....j.... .....@.. ..... @.....

File Icon

Icon Hash:	70d8ccd2d6ccf071

Static PE Info

General

Entrypoint:	0x48c76a
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:	0x6073F909 [Mon Apr 12 07:38:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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]
or dword ptr [edx], ecx
or eax, 00000020h
add byte ptr [ecx+49h], cl
sub al, byte ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
dec ebp
dec ebp
add byte ptr [edx], ch
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8c718	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8e000	0x36934	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	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	0x8a788	0x8a800	False	0.892861927459	data	7.83272627596	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x36934	0x36a00	False	0.368979726831	data	5.24988499022	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	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	0x8e310	0x94a9	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x977bc	0x4872	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x9c030	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	0xac858	0x94a8	data		
RT_ICON	0xb5d00	0x5488	data		
RT_ICON	0xbb188	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 16318463, next used block 4294909696		
RT_ICON	0xbf3b0	0x25a8	data		
RT_ICON	0xc1958	0x10a8	data		
RT_ICON	0xc2a00	0x988	data		
RT_ICON	0xc3388	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc37f0	0x92	data		
RT_GROUP_ICON	0xc3884	0x14	data		
RT_VERSION	0xc3898	0x374	data		
RT_MANIFEST	0xc3c0c	0xd25	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

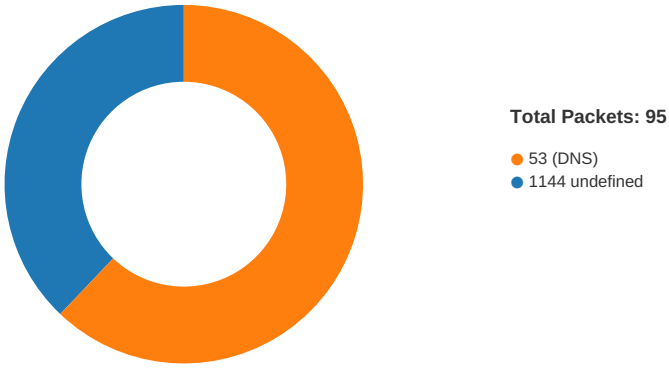
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Adobe Inc, Sel 2011 - 2021
Assembly Version	1.0.0.0
InternalName	Privilege.exe
FileVersion	1.0.0.0
CompanyName	Adobe Inc, Sel
LegalTrademarks	
Comments	
ProductName	Image Studio
ProductVersion	1.0.0.0
FileDescription	Image Studio
OriginalFilename	Privilege.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:00:01.355207920 CEST	49711	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:01.427133083 CEST	1144	49711	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:02.070334911 CEST	49711	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:02.142782927 CEST	1144	49711	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:02.757976055 CEST	49711	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:02.829590082 CEST	1144	49711	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:07.729110956 CEST	49713	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:07.805325031 CEST	1144	49713	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:08.477093935 CEST	49713	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:08.551440001 CEST	1144	49713	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:09.164709091 CEST	49713	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:09.238985062 CEST	1144	49713	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:13.256563902 CEST	49714	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:13.331157923 CEST	1144	49714	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:13.977611065 CEST	49714	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:14.051928997 CEST	1144	49714	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:14.665077925 CEST	49714	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:14.739634037 CEST	1144	49714	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:32.011816978 CEST	49718	1144	192.168.2.5	79.134.225.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:00:32.085053921 CEST	1144	49718	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:32.588512897 CEST	49718	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:32.659631014 CEST	1144	49718	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:33.166744947 CEST	49718	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:33.238087893 CEST	1144	49718	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:37.246861935 CEST	49719	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:37.323883057 CEST	1144	49719	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:37.838932991 CEST	49719	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:37.915091991 CEST	1144	49719	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:38.417068958 CEST	49719	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:38.491472006 CEST	1144	49719	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:42.498311043 CEST	49720	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:42.571405888 CEST	1144	49720	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:43.073781013 CEST	49720	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:43.147428036 CEST	1144	49720	79.134.225.30	192.168.2.5
Apr 12, 2021 13:00:43.651906967 CEST	49720	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:00:43.723453045 CEST	1144	49720	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:00.686086893 CEST	49728	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:00.757678986 CEST	1144	49728	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:01.262720108 CEST	49728	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:01.334613085 CEST	1144	49728	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:01.840920925 CEST	49728	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:01.915019035 CEST	1144	49728	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:05.920764923 CEST	49729	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:05.994015932 CEST	1144	49729	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:06.497595072 CEST	49729	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:06.569211960 CEST	1144	49729	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:07.075733900 CEST	49729	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:07.147341967 CEST	1144	49729	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:11.171880007 CEST	49730	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:11.247589111 CEST	1144	49730	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:11.747987986 CEST	49730	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:11.822231054 CEST	1144	49730	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:12.326163054 CEST	49730	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:12.402477980 CEST	1144	49730	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:29.445751905 CEST	49734	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:29.517343044 CEST	1144	49734	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:30.030828953 CEST	49734	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:30.102365017 CEST	1144	49734	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:30.608980894 CEST	49734	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:30.681199074 CEST	1144	49734	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:34.694035053 CEST	49735	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:34.765326023 CEST	1144	49735	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:35.265727043 CEST	49735	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:35.337838888 CEST	1144	49735	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:35.843965054 CEST	49735	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:35.917788029 CEST	1144	49735	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:39.925107956 CEST	49736	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:39.999701023 CEST	1144	49736	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:40.500411987 CEST	49736	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:40.576354980 CEST	1144	49736	79.134.225.30	192.168.2.5
Apr 12, 2021 13:01:41.078603983 CEST	49736	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 13:01:41.154787064 CEST	1144	49736	79.134.225.30	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:59:38.604585886 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:38.754195929 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:38.802927971 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:38.936371088 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:38.987447023 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:39.106429100 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:39.149488926 CEST	61805	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:59:39.155225039 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:39.211309910 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:40.069293976 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:40.121340990 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:41.078735113 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:41.138041973 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:42.030767918 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:42.083446980 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:42.835169077 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:42.897017956 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:44.331366062 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:44.383035898 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:45.297561884 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:45.350640059 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:46.365259886 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:46.414057970 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:47.401859045 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:47.453624964 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:48.648853064 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:48.697606087 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:51.815304995 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:51.865305901 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 12:59:52.923866987 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 12, 2021 12:59:52.977523088 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:02.023041010 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:02.081365108 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:14.522727013 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:14.578665018 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:18.837311029 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:18.895767927 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:18.998567104 CEST	60075	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:00:19.058829069 CEST	53	60075	8.8.4.4	192.168.2.5
Apr 12, 2021 13:00:19.073870897 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:19.131177902 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:22.693537951 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:22.752840996 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:23.198050022 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:23.255831957 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:23.294791937 CEST	54791	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:00:23.346416950 CEST	53	54791	8.8.4.4	192.168.2.5
Apr 12, 2021 13:00:23.647906065 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:23.710222960 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:27.754089117 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:27.815674067 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:27.830712080 CEST	58530	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:00:27.887969017 CEST	53	58530	8.8.4.4	192.168.2.5
Apr 12, 2021 13:00:27.939367056 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:27.989912033 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:47.817176104 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:47.874506950 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:47.920762062 CEST	57344	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:00:47.972507954 CEST	53	57344	8.8.4.4	192.168.2.5
Apr 12, 2021 13:00:48.013180971 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:48.072132111 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:52.117523909 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:52.180938005 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:52.204854965 CEST	57151	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:00:52.265489101 CEST	53	57151	8.8.4.4	192.168.2.5
Apr 12, 2021 13:00:52.326237917 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:52.381699085 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:52.625020981 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:52.676872969 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:56.459278107 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:56.518841028 CEST	53	51649	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:00:56.526599884 CEST	65086	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:56.548965931 CEST	56432	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:00:56.591074944 CEST	53	65086	8.8.8.8	192.168.2.5
Apr 12, 2021 13:00:56.602674007 CEST	53	56432	8.8.4.4	192.168.2.5
Apr 12, 2021 13:00:56.611700058 CEST	52929	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:00:56.671649933 CEST	53	52929	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:13.993594885 CEST	64317	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:14.053746939 CEST	53	64317	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:16.437031031 CEST	61004	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:16.496603012 CEST	53	61004	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:16.499430895 CEST	56895	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:01:16.556838036 CEST	53	56895	8.8.4.4	192.168.2.5
Apr 12, 2021 13:01:16.663183928 CEST	62372	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:16.724874020 CEST	53	62372	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:20.775239944 CEST	61515	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:20.832735062 CEST	53	61515	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:20.838588953 CEST	56675	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:01:20.903629065 CEST	53	56675	8.8.4.4	192.168.2.5
Apr 12, 2021 13:01:20.946317911 CEST	57172	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:21.003734112 CEST	53	57172	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:25.042305946 CEST	55267	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:25.100878000 CEST	53	55267	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:25.128623962 CEST	50969	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:01:25.188944101 CEST	53	50969	8.8.4.4	192.168.2.5
Apr 12, 2021 13:01:25.383774042 CEST	64362	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:25.432615995 CEST	53	64362	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:26.924032927 CEST	54766	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:26.973036051 CEST	53	54766	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:28.715754032 CEST	61446	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:28.783889055 CEST	53	61446	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:45.203002930 CEST	57515	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:45.261925936 CEST	53	57515	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:45.405416965 CEST	58199	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:01:45.462657928 CEST	53	58199	8.8.4.4	192.168.2.5
Apr 12, 2021 13:01:45.478410959 CEST	65221	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:45.536000013 CEST	53	65221	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:49.592000961 CEST	61573	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:49.643600941 CEST	53	61573	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:49.674961090 CEST	56562	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:01:49.725357056 CEST	53	56562	8.8.4.4	192.168.2.5
Apr 12, 2021 13:01:49.895150900 CEST	53591	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:49.945727110 CEST	53	53591	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:53.955430031 CEST	59688	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:54.015872002 CEST	53	59688	8.8.8.8	192.168.2.5
Apr 12, 2021 13:01:54.018208981 CEST	56032	53	192.168.2.5	8.8.4.4
Apr 12, 2021 13:01:54.077900887 CEST	53	56032	8.8.4.4	192.168.2.5
Apr 12, 2021 13:01:54.080919027 CEST	61150	53	192.168.2.5	8.8.8.8
Apr 12, 2021 13:01:54.140571117 CEST	53	61150	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 13:00:18.837311029 CEST	192.168.2.5	8.8.8.8	0x9314	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:18.998567104 CEST	192.168.2.5	8.8.4.4	0xf60	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:19.073870897 CEST	192.168.2.5	8.8.8.8	0xc20e	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:23.198050022 CEST	192.168.2.5	8.8.8.8	0x106	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:23.294791937 CEST	192.168.2.5	8.8.4.4	0xb945	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:23.647906065 CEST	192.168.2.5	8.8.8.8	0xefbc	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:27.754089117 CEST	192.168.2.5	8.8.8.8	0x70c8	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 13:00:27.830712080 CEST	192.168.2.5	8.8.4.4	0x73e0	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:27.939367056 CEST	192.168.2.5	8.8.8.8	0x648	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:47.817176104 CEST	192.168.2.5	8.8.8.8	0xff48	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:47.920762062 CEST	192.168.2.5	8.8.4.4	0xff03	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:48.013180971 CEST	192.168.2.5	8.8.8.8	0x67d2	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:52.117523909 CEST	192.168.2.5	8.8.8.8	0x91a6	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:52.204854965 CEST	192.168.2.5	8.8.4.4	0x6b41	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:52.326237917 CEST	192.168.2.5	8.8.8.8	0x706a	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:56.459278107 CEST	192.168.2.5	8.8.8.8	0xc33	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:56.548965931 CEST	192.168.2.5	8.8.4.4	0xc7c9	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:56.611700058 CEST	192.168.2.5	8.8.8.8	0x7f39	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:16.437031031 CEST	192.168.2.5	8.8.8.8	0x22fa	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:16.499430895 CEST	192.168.2.5	8.8.4.4	0xfbf7	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:16.663183928 CEST	192.168.2.5	8.8.8.8	0x449b	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:20.775239944 CEST	192.168.2.5	8.8.8.8	0xe506	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:20.838588953 CEST	192.168.2.5	8.8.4.4	0xf0fc	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:20.946317911 CEST	192.168.2.5	8.8.8.8	0xd863	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:25.042305946 CEST	192.168.2.5	8.8.8.8	0xcfb1	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:25.128623962 CEST	192.168.2.5	8.8.4.4	0xc4b0	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:25.383774042 CEST	192.168.2.5	8.8.8.8	0x80d2	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:45.203002930 CEST	192.168.2.5	8.8.8.8	0x75c5	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:45.405416965 CEST	192.168.2.5	8.8.4.4	0x5a49	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:45.478410959 CEST	192.168.2.5	8.8.8.8	0x9df2	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:49.592000961 CEST	192.168.2.5	8.8.8.8	0xc449	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:49.674961090 CEST	192.168.2.5	8.8.4.4	0xa5b3	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:49.895150900 CEST	192.168.2.5	8.8.8.8	0x77e0	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:53.955430031 CEST	192.168.2.5	8.8.8.8	0x1c57	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:54.018208981 CEST	192.168.2.5	8.8.4.4	0x9d98	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:54.080919027 CEST	192.168.2.5	8.8.8.8	0xec79	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 13:00:18.895767927 CEST	8.8.8.8	192.168.2.5	0x9314	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:19.058829069 CEST	8.8.4.4	192.168.2.5	0xf60	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:19.131177902 CEST	8.8.8.8	192.168.2.5	0xc20e	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:23.255831957 CEST	8.8.8.8	192.168.2.5	0x106	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

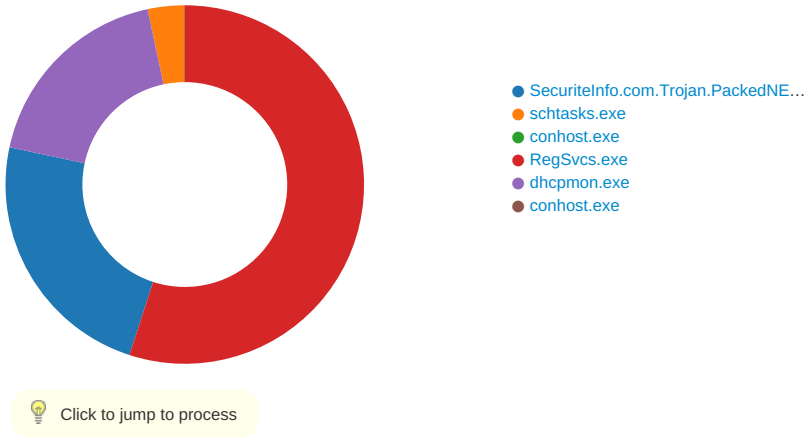
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 13:00:23.346416950 CEST	8.8.4.4	192.168.2.5	0xb945	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:23.710222960 CEST	8.8.8.8	192.168.2.5	0xefbc	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:27.815674067 CEST	8.8.8.8	192.168.2.5	0x70c8	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:27.887969017 CEST	8.8.4.4	192.168.2.5	0x73e0	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:27.989912033 CEST	8.8.8.8	192.168.2.5	0x648	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:47.874506950 CEST	8.8.8.8	192.168.2.5	0xff48	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:47.972507954 CEST	8.8.4.4	192.168.2.5	0xff03	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:48.072132111 CEST	8.8.8.8	192.168.2.5	0x67d2	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:52.180938005 CEST	8.8.8.8	192.168.2.5	0x91a6	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:52.265489101 CEST	8.8.4.4	192.168.2.5	0x6b41	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:52.381699085 CEST	8.8.8.8	192.168.2.5	0x706a	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:56.518841028 CEST	8.8.8.8	192.168.2.5	0xc33	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:56.602674007 CEST	8.8.4.4	192.168.2.5	0xc7c9	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:00:56.671649933 CEST	8.8.8.8	192.168.2.5	0x7f39	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:16.496603012 CEST	8.8.8.8	192.168.2.5	0x22fa	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:16.556838036 CEST	8.8.4.4	192.168.2.5	0xfbf7	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:16.724874020 CEST	8.8.8.8	192.168.2.5	0x449b	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:20.832735062 CEST	8.8.8.8	192.168.2.5	0xe506	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:20.903629065 CEST	8.8.4.4	192.168.2.5	0xf0fc	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:21.003734112 CEST	8.8.8.8	192.168.2.5	0xd863	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:25.100878000 CEST	8.8.8.8	192.168.2.5	0xcfb1	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:25.188944101 CEST	8.8.4.4	192.168.2.5	0xc4b0	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:25.432615995 CEST	8.8.8.8	192.168.2.5	0x80d2	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:45.261925936 CEST	8.8.8.8	192.168.2.5	0x75c5	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:45.462657928 CEST	8.8.4.4	192.168.2.5	0x5a49	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:45.536000013 CEST	8.8.8.8	192.168.2.5	0x9df2	Name error (3)	nassiru115 5.ddns.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 13:01:49.643600941 CEST	8.8.8.8	192.168.2.5	0xc449	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:49.725357056 CEST	8.8.4.4	192.168.2.5	0xa5b3	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:49.945727110 CEST	8.8.8.8	192.168.2.5	0x77e0	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:54.015872002 CEST	8.8.8.8	192.168.2.5	0x1c57	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:54.077900887 CEST	8.8.4.4	192.168.2.5	0x9d98	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:01:54.140571117 CEST	8.8.8.8	192.168.2.5	0xec79	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.PackedNET.645.23105.exe PID: 6484
Parent PID: 5792

General

Start time:	12:59:46
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe'
Imagebase:	0x1b0000
File size:	792064 bytes
MD5 hash:	6A647FD057FD6A0B85C644D928125EB4

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.262202622.0000000003AB1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.262202622.0000000003AB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.262202622.0000000003AB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.261175350.0000000002AB1000.00000004.00000001.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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\blFUun.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	4D518B4	CopyFileW
C:\Users\user\AppData\Roaming\blFUun.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	4D518B4	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF1BB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	72119869	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF1BB.tmp	success or wait	1	4D52622	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\blFUun.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 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 09 f9 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 a8 08 00 00 6c 03 00 00 00 00 00 6a c7 08 00 00 20 00 00 00 e0 08 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 80 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.....s`.......... ....P......l......j.... ....@.. ....@................	success or wait	4	4D518B4	CopyFileW
C:\Users\user\AppData\Roaming\blFUun.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	4D518B4	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF1BB.tmp	unknown	1643	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 37 37 31 5c 61 6c 66 6f 6e 73 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	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationI	success or wait	1	4D522DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.645.23105.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: schtasks.exe PID: 6704 Parent PID: 6484

General

Start time:	12:59:57
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\blFUun' /XML 'C:\Users\user\AppData\Local\Temp\tmpF1BB.tmp'
Imagebase:	0x820000
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\tmpF1BB.tmp	unknown	2	success or wait	1	82AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF1BB.tmp	unknown	1644	success or wait	1	82ABD9	ReadFile

Analysis Process: conhost.exe PID: 6724 Parent PID: 6704

General

Start time:	12:59:58
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RegSvcs.exe PID: 6840 Parent PID: 6484

General

Start time:	12:59:58
Start date:	12/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x510000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.508372796.0000000004FD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.508372796.0000000004FD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.500192015.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.500192015.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.500192015.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.508666982.0000000005420000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.508666982.0000000005420000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.508666982.0000000005420000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.507210051.0000000003C2B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.507210051.0000000003C2B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	28607A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	286089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	28607A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	2860B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	28607A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	28607A1	CreateDirectoryW
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	72B860AC	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	72B860AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	5b 6a b7 8d ed fd d8 48	[j.....H	success or wait	1	2860A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	32768	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 80 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 cf ce 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 b1 5b 01 00 03 00 40 05 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..... {Z.................P... ....k... ....@.. ....[....@.................	success or wait	1	2860B20	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2860A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	2860A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	2860A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	72C5BF06	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	2860C12	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 6316 Parent PID: 3472

General

Start time:	13:00:11
Start date:	12/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x420000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7219DCB3	unknown
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	7219DFAB	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target applicat ion, error if it already exist s... /exapp	success or wait	3	7219DFAB	unknown
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	7219DFAB	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 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	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: conhost.exe PID: 5760 Parent PID: 6316

General

Start time:	13:00:11
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis