ID: 624197
Sample Name:
SecuriteInfo.com.Trojan.PackedNET.331.28355.4334
Cookbook: default.jbs
Time: 10:40:22
Date: 11/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

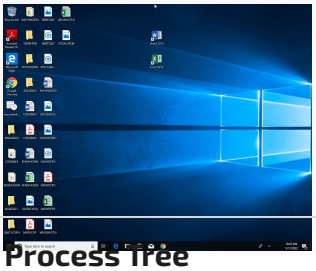
Windows Analysis Report

SecuriteInfo.com.Trojan.PackedNET.331.28355.4334

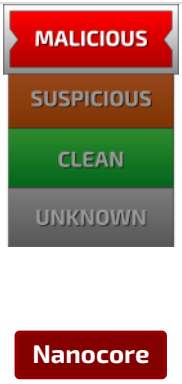
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.PackedNET.331.28355.4334 (renamed file extension from 4334 to exe)
Analysis ID:	624197
MD5:	1f04c12ab3a22f6..
SHA1:	9913975b167b01..
SHA256:	de42477eb270c4..
Tags:	exe
Infos:	



Detection



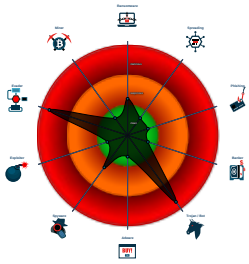
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.PackedNET.331.28355.exe (PID: 5012 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.331.28355.exe" MD5: 1F04C12AB3A22F6806D30BACB7552F19)
  - RegSvcs.exe (PID: 4736 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 6792 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "484915e0-ae38-4675-9bf6-0f4a5bd5",
  "Domain1": "youngnonte.hopto.org",
  "Domain2": "91.193.75.133",
  "Port": 2323,
  "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 Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.408831258.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000000.408831258.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000000.408831258.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000004.00000000.409213843.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000000.409213843.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 31 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.5e30000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.5e30000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
4.2.RegSvcs.exe.5e30000.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
4.2.RegSvcs.exe.5e30000.6.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin • 0x147a2:$s6: get_ClientSettings
4.2.RegSvcs.exe.3c58a48.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 78 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133 −

Timestamp:	192.168.2.791.193.75.1334979723232816718 05/11/22-10:42:39.036019
SID:	2816718
Source Port:	49797
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133 −

Timestamp:	192.168.2.791.193.75.1334985723232816766 05/11/22-10:43:23.924010
SID:	2816766
Source Port:	49857
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133 −

Timestamp:	192.168.2.791.193.75.1334987523232816766 05/11/22-10:43:44.394960
SID:	2816766
Source Port:	49875
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334986923232816766 05/11/22-10:43:31.252983
SID:	2816766
Source Port:	49869
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334979723232816766 05/11/22-10:42:39.036019
SID:	2816766
Source Port:	49797
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334982123232816766 05/11/22-10:43:17.029709
SID:	2816766
Source Port:	49821
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334980323232816766 05/11/22-10:42:46.018391
SID:	2816766
Source Port:	49803
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334980923232816766 05/11/22-10:43:06.473922
SID:	2816766
Source Port:	49809
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334987323232816766 05/11/22-10:43:38.940134
SID:	2816766
Source Port:	49873
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334978723232816766 05/11/22-10:42:24.860231
SID:	2816766
Source Port:	49787
Destination Port:	2323

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334980723232816766 05/11/22-10:42:53.078454
SID:	2816766
Source Port:	49807
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334977723232816766 05/11/22-10:42:09.828204
SID:	2816766
Source Port:	49777
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334987323232816718 05/11/22-10:43:38.940134
SID:	2816718
Source Port:	49873
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334979423232816766 05/11/22-10:42:31.876458
SID:	2816766
Source Port:	49794
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 91.193.75.133 - Destination IP: 192.168.2.7	
Timestamp:	91.193.75.133192.168.2.72323498212810290 05/11/22-10:43:15.841800
SID:	2810290
Source Port:	2323
Destination Port:	49821
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334978223232816766 05/11/22-10:42:17.828455
SID:	2816766
Source Port:	49782
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 91.193.75.133	
Timestamp:	192.168.2.791.193.75.1334980823232816766 05/11/22-10:43:00.269339
SID:	2816766
Source Port:	49808
Destination Port:	2323
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

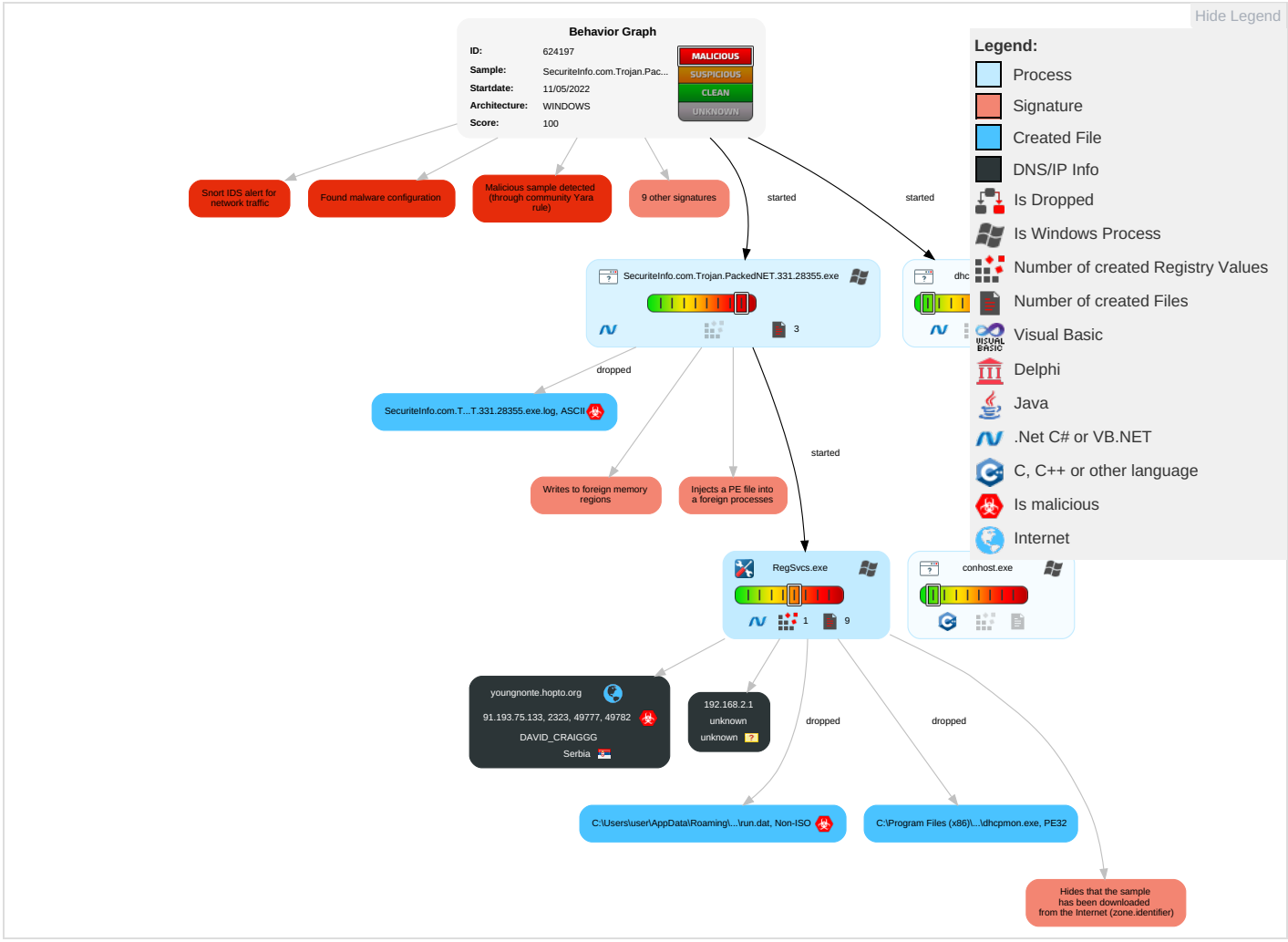
Detected Nanocore Rat

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	2 1 2 Process Injection	2 Masquerading	1 1 Input Capture	1 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

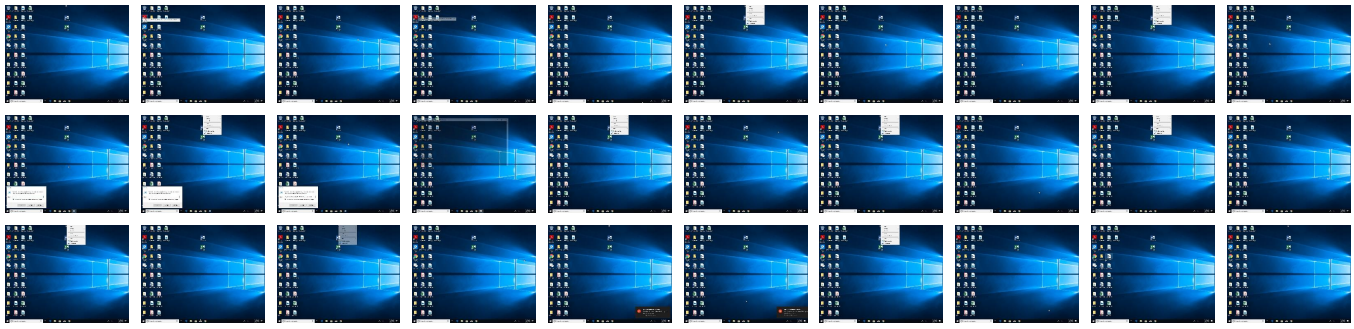
Behavior Graph



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.331.28355.exe	32%	ReversingLabs	Win32.Trojan.Pwsx	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegSvcs.exe.5e30000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
4.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
4.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
youngnonte.hopto.org	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://go.microsoft.c#	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
91.193.75.133	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
youngnonte.hopto.org	91.193.75.133	true	true		unknown

Contacted URLs

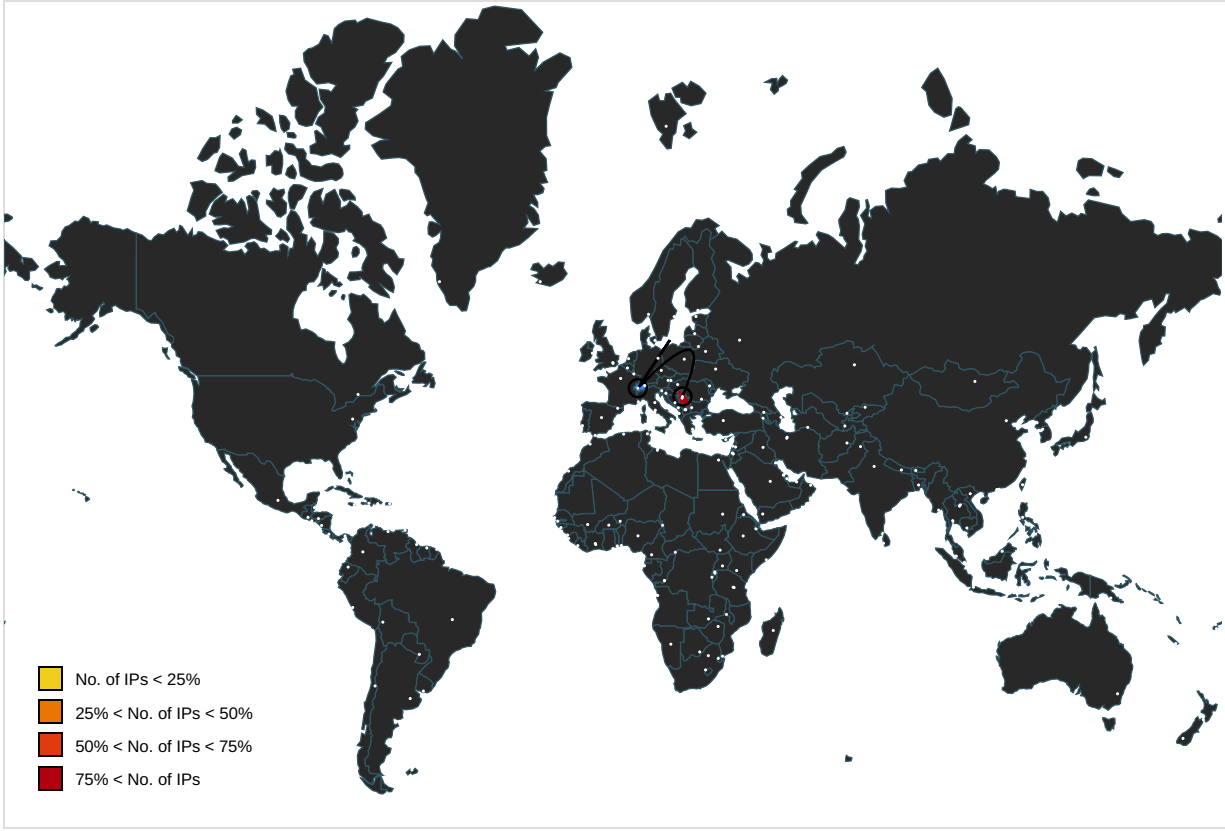
Name	Malicious	Antivirus Detection	Reputation
youngnonte.hopto.org	true	• Avira URL Cloud: safe	unknown
91.193.75.133	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://go.microsoft.c#	dhcpmon.exe, 00000008.00000002.444043931.0000000001642000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Trojan.PackedNET.331.28355.exe, 00000000.00000002.419340426.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.193.75.133	youngnonte.hopto.org	Serbia		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624197
Start date and time: 11/05/202210:40:22	2022-05-11 10:40:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.PackedNET.331.28355.4334 (renamed file extension from 4334 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:	23
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@5/6@14/2

EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.9%) • Quality average: 100% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fp-afd.azureedge.us, client.wns.windows.com, fs.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, b-ring.msedge.net, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, fp-vp.azureedge.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target dhcpmon.exe, PID 6792 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:41:52	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.PackedNET.331.28355.exe modified
10:42:06	API Interceptor	805x Sleep call for process: RegSvcs.exe modified
10:42:07	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|....P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.331.28355.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.331.28355.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data

Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35 A5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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:Ftn:Ftn
MD5:	9E0F3049136E4ABE28D27EE1B11D0884
SHA1:	2A5E18BB091286E43CD954AF4D421D78CE042A7C
SHA-256:	86880178E275C92A02FA7EC15A1626618DE00FCE75EA83600F79C39E2AAAAC37
SHA-512:	7EA88728E379BF9F73DF01F18B0F8A8C70F5FACB7234D9DF1B1E498FE7B5B3021C998BEA2378A59B39D12396254A3C3B4BF77D7B772C3716667501753D1564CE
Malicious:	**true**
Preview:	.>..u3.H

\Device\ConDrv

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141 5
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, 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... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.026942711928976

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.331.28355.exe
File size:	1173504
MD5:	1f04c12ab3a22f6806d30bacb7552f19
SHA1:	9913975b167b01b96364cad477ca6dfab71da454
SHA256:	de42477eb270c42a2eaf57e6efb465263fc02e72e6c8442fdbd27aa3bd8e76a5
SHA512:	2b95be12e4df50eeb09b950e31ae7003ba1fe540475cd32cd5e4260e59fdbeab8e6378ed457d43ab1142b1bf40e23ec20c849065bb103b79b0179bfd1b8ac274
SSDEEP:	12288:m+Cenfxt7J00Fq6j/wXgl4NV77zvRE2hEr5hHeC5ROGFmTDcvvj6yVBJGen0ni+f:mZg20Fbo7/762hM5hPTmTAL
TLSH:	E24528987254F5DEC85BD071CE685CF0AA207C66C32B820B50173D9DB97EA83DF219B6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Czb.....0.....Z..... .....@.. .....@.....@.....

File Icon

Icon Hash:	f274fec6b6c2e00c

Static PE Info

General

Entrypoint:	0x50aace
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:	0x627A439B [Tue May 10 10:51:07 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10aa78	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10c000	0x15718	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x122000	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	0x108ad4	0x108c00	False	0.649346745161	data	7.16329250729	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0x15718	0x15800	False	0.151662427326	data	4.00324413901	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x122000	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	0x10c1d8	0x8a8	data		
RT_ICON	0x10ca80	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x10cfe8	0x10828	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x11d810	0x25a8	data		
RT_ICON	0x11fdb8	0x10a8	data		
RT_ICON	0x120e60	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1212c8	0x5a	data		
RT_VERSION	0x121324	0x3f4	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011 BASeCamp Software Solutions
Assembly Version	1.4.8.0
InternalName	TypeLoadExceptionHol.exe
FileVersion	1.4.8.0
CompanyName	BASeCamp Software Solutions
LegalTrademarks	
Comments	
ProductName	BASeCamp JobClock
ProductVersion	1.4.8.0
FileDescription	JobClock Administration Applet
OriginalFilename	TypeLoadExceptionHol.exe

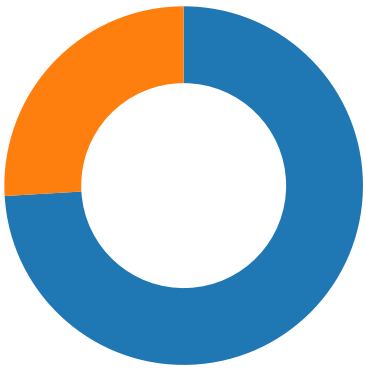
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.791.193.75.133 4979723232816718 05/11/22-10:42:39.036019	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49797	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4985723232816766 05/11/22-10:43:23.924010	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49857	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4987523232816766 05/11/22-10:43:44.394960	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49875	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4986923232816766 05/11/22-10:43:31.252983	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49869	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4979723232816766 05/11/22-10:42:39.036019	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49797	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4982123232816766 05/11/22-10:43:17.029709	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49821	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4980323232816766 05/11/22-10:42:46.018391	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49803	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4980923232816766 05/11/22-10:43:06.473922	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49809	2323	192.168.2.7	91.193.75.133

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.791.193.75.133 4987323232816766 05/11/22-10:43:38.940134	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49873	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4978723232816766 05/11/22-10:42:24.860231	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49787	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4980723232816766 05/11/22-10:42:53.078454	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49807	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4977723232816766 05/11/22-10:42:09.828204	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49777	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4987323232816718 05/11/22-10:43:38.940134	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49873	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4979423232816766 05/11/22-10:42:31.876458	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49794	2323	192.168.2.7	91.193.75.133
91.193.75.133192.168.2.7 2323498212810290 05/11/22-10:43:15.841800	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	2323	49821	91.193.75.133	192.168.2.7
192.168.2.791.193.75.133 4978223232816766 05/11/22-10:42:17.828455	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49782	2323	192.168.2.7	91.193.75.133
192.168.2.791.193.75.133 4980823232816766 05/11/22-10:43:00.269339	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49808	2323	192.168.2.7	91.193.75.133

Network Port Distribution



Total Packets: 54

- 53 (DNS)
- 2323 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:42:07.884488106 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:08.101824045 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:08.101926088 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:08.289627075 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:08.561732054 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:08.702646971 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:08.717859983 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:08.949024916 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:08.951173067 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.218835115 CEST	2323	49777	91.193.75.133	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:42:09.366214037 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.628810883 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.630662918 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.632252932 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.634701014 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.636718035 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.636847019 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.640805006 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.643790960 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.643906116 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.647773027 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.651766062 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.651940107 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.659866095 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.667797089 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.668570042 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.828203917 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.868817091 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.869220018 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.878812075 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.878846884 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.878871918 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.879038095 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.879064083 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.879998922 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.880110979 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.881819963 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.882283926 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.884793043 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.884953022 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.886666059 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.887518883 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.889000893 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.891669989 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.891810894 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.892244101 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.896337986 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.896538973 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.900554895 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.901788950 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.902044058 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.907888889 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.907967091 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.909468889 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.910161972 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.917926073 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.917952061 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.918090105 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.924743891 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.924767017 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.924783945 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:09.924873114 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:09.925044060 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.107511044 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.111494064 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.111659050 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.112443924 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.112489939 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.113070965 CEST	49777	2323	192.168.2.7	91.193.75.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:42:10.117878914 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.119751930 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.120070934 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.127706051 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.127760887 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.127885103 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.127943039 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.137955904 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.137998104 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.138148069 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.144026041 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.144138098 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.148011923 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.148899078 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.149030924 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.152810097 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.152846098 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.152901888 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.160171032 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.163289070 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.163321018 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.163376093 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.164191008 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.164293051 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.165267944 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.167901039 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.168031931 CEST	49777	2323	192.168.2.7	91.193.75.133
May 11, 2022 10:42:10.177052975 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.177100897 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.177129030 CEST	2323	49777	91.193.75.133	192.168.2.7
May 11, 2022 10:42:10.177254915 CEST	49777	2323	192.168.2.7	91.193.75.133

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:42:07.846601009 CEST	50519	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:07.867922068 CEST	53	50519	8.8.8.8	192.168.2.7
May 11, 2022 10:42:15.350569963 CEST	54143	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:15.369637966 CEST	53	54143	8.8.8.8	192.168.2.7
May 11, 2022 10:42:22.935004950 CEST	52480	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:22.954726934 CEST	53	52480	8.8.8.8	192.168.2.7
May 11, 2022 10:42:29.905711889 CEST	50125	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:29.927062035 CEST	53	50125	8.8.8.8	192.168.2.7
May 11, 2022 10:42:37.024189949 CEST	65214	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:37.043608904 CEST	53	65214	8.8.8.8	192.168.2.7
May 11, 2022 10:42:44.090857029 CEST	62843	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:44.109671116 CEST	53	62843	8.8.8.8	192.168.2.7
May 11, 2022 10:42:51.063699961 CEST	59946	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:51.082979918 CEST	53	59946	8.8.8.8	192.168.2.7
May 11, 2022 10:42:58.456557035 CEST	60920	53	192.168.2.7	8.8.8.8
May 11, 2022 10:42:58.477355957 CEST	53	60920	8.8.8.8	192.168.2.7
May 11, 2022 10:43:05.366317034 CEST	51160	53	192.168.2.7	8.8.8.8
May 11, 2022 10:43:05.385807991 CEST	53	51160	8.8.8.8	192.168.2.7
May 11, 2022 10:43:15.109352112 CEST	49495	53	192.168.2.7	8.8.8.8
May 11, 2022 10:43:15.128709078 CEST	53	49495	8.8.8.8	192.168.2.7
May 11, 2022 10:43:21.949346066 CEST	62837	53	192.168.2.7	8.8.8.8
May 11, 2022 10:43:21.971178055 CEST	53	62837	8.8.8.8	192.168.2.7
May 11, 2022 10:43:28.166333914 CEST	51516	53	192.168.2.7	8.8.8.8
May 11, 2022 10:43:28.185709953 CEST	53	51516	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:43:36.466886044 CEST	64521	53	192.168.2.7	8.8.8.8
May 11, 2022 10:43:36.487708092 CEST	53	64521	8.8.8.8	192.168.2.7
May 11, 2022 10:43:43.429339886 CEST	49198	53	192.168.2.7	8.8.8.8
May 11, 2022 10:43:43.447773933 CEST	53	49198	8.8.8.8	192.168.2.7

DNS Queries

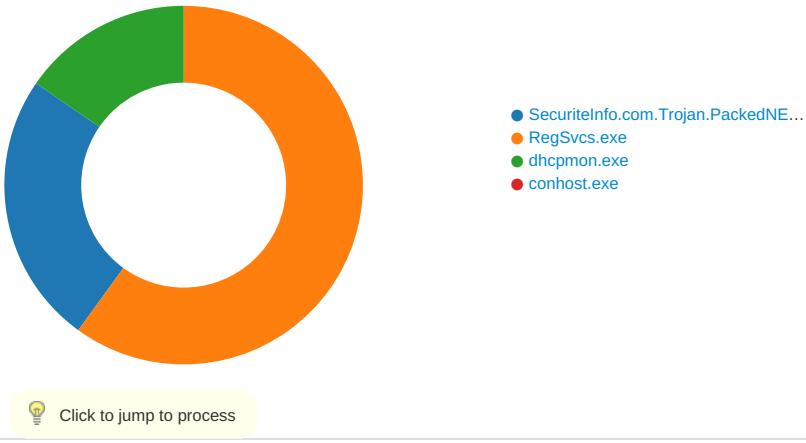
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2022 10:42:07.846601009 CEST	192.168.2.7	8.8.8.8	0x3026	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:42:15.350569963 CEST	192.168.2.7	8.8.8.8	0xef57	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:42:22.935004950 CEST	192.168.2.7	8.8.8.8	0x7a53	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:42:29.905711889 CEST	192.168.2.7	8.8.8.8	0x8cdf	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:42:37.024189949 CEST	192.168.2.7	8.8.8.8	0x373b	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:42:44.090857029 CEST	192.168.2.7	8.8.8.8	0x2b83	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:42:51.063699961 CEST	192.168.2.7	8.8.8.8	0xa6c6	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:42:58.456557035 CEST	192.168.2.7	8.8.8.8	0x6f9c	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:43:05.366317034 CEST	192.168.2.7	8.8.8.8	0x7267	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:43:15.109352112 CEST	192.168.2.7	8.8.8.8	0x881c	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:43:21.949346066 CEST	192.168.2.7	8.8.8.8	0x1d62	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:43:28.166333914 CEST	192.168.2.7	8.8.8.8	0xccd9	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:43:36.466886044 CEST	192.168.2.7	8.8.8.8	0xc95d	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)
May 11, 2022 10:43:43.429339886 CEST	192.168.2.7	8.8.8.8	0x78f5	Standard query (0)	youngnonte .hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2022 10:42:07.867922068 CEST	8.8.8.8	192.168.2.7	0x3026	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:42:15.369637966 CEST	8.8.8.8	192.168.2.7	0xef57	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:42:22.954726934 CEST	8.8.8.8	192.168.2.7	0x7a53	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:42:29.927062035 CEST	8.8.8.8	192.168.2.7	0x8cdf	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:42:37.043608904 CEST	8.8.8.8	192.168.2.7	0x373b	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:42:44.109671116 CEST	8.8.8.8	192.168.2.7	0x2b83	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:42:51.082979918 CEST	8.8.8.8	192.168.2.7	0xa6c6	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:42:58.477355957 CEST	8.8.8.8	192.168.2.7	0x6f9c	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:43:05.385807991 CEST	8.8.8.8	192.168.2.7	0x7267	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:43:15.128709078 CEST	8.8.8.8	192.168.2.7	0x881c	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:43:21.971178055 CEST	8.8.8.8	192.168.2.7	0x1d62	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:43:28.185709953 CEST	8.8.8.8	192.168.2.7	0xccd9	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:43:36.487708092 CEST	8.8.8.8	192.168.2.7	0xc95d	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)
May 11, 2022 10:43:43.447773933 CEST	8.8.8.8	192.168.2.7	0x78f5	No error (0)	youngnonte .hopto.org		91.193.75.133	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.PackedNET.331.28355.exe PID: 5012, Parent PID: 792

General

Target ID:	0
Start time:	10:41:39
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.331.28355.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.331.28355.exe"
Imagebase:	0x960000
File size:	1173504 bytes
MD5 hash:	1F04C12AB3A22F6806D30BACB7552F19
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.415299432.0000000002EE8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.414167821.0000000002D81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.416862550.0000000003F52000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.416862550.0000000003F52000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.416862550.0000000003F52000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD2CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DD2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.331.28355.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E03C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.331.28355.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E03C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C191B4F	ReadFile

Analysis Process: RegSvcs.exe PID: **4736**, Parent PID: **5012**

General

Target ID:	4
Start time:	10:42:01
Start date:	11/05/2022

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x8d0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000004.00000000.408831258.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.408831258.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.408831258.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.409213843.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.409213843.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.409213843.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.631819376.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.631819376.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.631819376.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.631819376.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.408232276.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.408232276.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.408232276.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.629684099.0000000003C51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.626920584.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.626920584.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.626920584.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.628123506.0000000002BF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.631747506.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.631747506.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000004.00000002.631747506.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.409721909.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.409721909.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.409721909.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

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	6DD2CF06	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	6DD2CF06	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	6C19BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6C191E60	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	6C19BEFF	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	6C19DD66	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	6C19BEFF	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	6C19BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	14	6C191E60	CreateFileW

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	0	8	fd 3e fd fd 75 33 fd 48	>u3H	success or wait	1	6C191B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 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.$PELzXZ0dV @ "`	success or wait	1	6C19DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	14	6C191B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DD0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DCED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DCED72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6DCED72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6DCED72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DD05705	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DCED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DCED72F	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	6C19646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **6792**, Parent PID: **3808**

General

Target ID:	8
Start time:	10:42:16
Start date:	11/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x7ff7e8070000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E03C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C191B4F	WriteFile
\Device\ConDrv	141	141	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 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67	USAGE: regsvcs.exe [options] AssemblyNameOptions: /? or /help Display this usage message. /fc Find or create targ	success or wait	1	6C191B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	397	256	20 20 20 20 20 20 20 20 45 78 70 65 63 74 20 61 6e 20 65 78 69 73 74 69 6e 67 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 74 6c 62 3a 3c 74 6c 62 66 69 6c 65 3e 20 20 46 69 6c 65 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 65 78 70 6f 72 74 65 64 20 74 79 70 65 20 6c 69 62 72 61 72 79 2e 0d 0a 20 20 20 20 20 2f 61 70 70 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f 70 61 72 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 6f 72 20 69 64 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 70 61 72 74 69 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f	Expect an existing application. /tlb:<tlbfile> Filename for the exported type library. /appname: <name> Use the specified name for the t arget application. /parname:<name> Use the specified name or id for the target partition. /	success or wait	3	6C191B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C191B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 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 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	6E03C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile

Analysis Process: conhost.exe PID: **5536**, Parent PID: **6792**

General

Target ID:	9
Start time:	10:42:17
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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

No disassembly