ID: 796996
Sample Name: Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
Cookbook: default.jbs
Time: 13:51:27
Date: 02/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

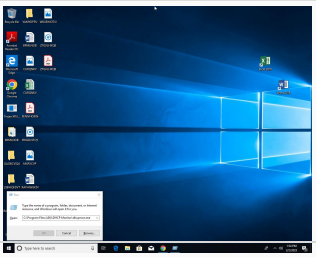
Windows Analysis Report

Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe

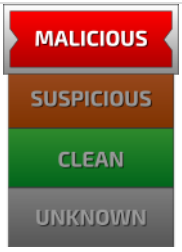
Overview

General Information

Sample Name:	Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
Analysis ID:	796996
MD5:	e587236cb6e5…
SHA1:	8b9f158fd574c…
SHA256:	249a4af8064c5…
Tags:	exe NanoCore RAT
Infos:	



Detection



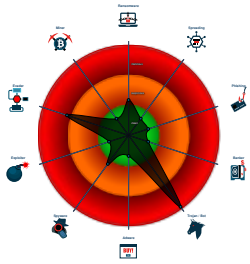
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic

Classification



Process Tree

- **System is w10x64**
- Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe (PID: 5044 cmdline: C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe MD5: E587236CB6E5CCF2497AB08B245F724F)
  - schtasks.exe (PID: 2472 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp2F6A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4852 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp315F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe (PID: 1244 cmdline: C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe 0 MD5: E587236CB6E5CCF2497AB08B245F724F)
- dhcpmon.exe (PID: 2148 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: E587236CB6E5CCF2497AB08B245F724F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Group": "KUWAIT",
  "Domain1": "doc4.ddns.net",
  "Domain2": "donald30m.gleeze.com",
  "Port": 9497,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected

Source	Rule	Description	Author	Strings
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xff8d:$a1: NanoCore.ClientPluginHost • 0xff4d:$a2: NanoCore.ClientPlugin • 0x11ea6:$b1: get_BuilderSettings • 0xfda9:$b2: ClientLoaderForm.resources • 0x115c6:$b3: PluginCommand • 0xff7e:$b4: IClientAppHost • 0x1a3fe:$b5: GetBlockHash • 0x124fe:$b6: AddHostEntry • 0x161f1:$b7: LogClientException • 0x1246b:$b8: PipeExists • 0xffb7:$b9: IClientLoggingHost
00000000.00000002.584551400.00000000055C0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.2af3f10.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.2af3f10.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
5.2.Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.2af3f10.0.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
5.2.Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.2af3f10.0.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
6.2.dhcpmon.exe.3483dc4.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
Click to see the 53 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118

Timestamp:	192.168.2.5216.218.135.1184970494972025019 02/02/23-13:52:37.416548
SID:	2025019
Source Port:	49704
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118

Timestamp:	192.168.2.5216.218.135.1184971494972025019 02/02/23-13:53:43.248786
SID:	2025019
Source Port:	49714
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118

Timestamp:	192.168.2.5216.218.135.1184970494972816718 02/02/23-13:52:37.610379
SID:	2816718
Source Port:	49704
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118

Timestamp:	192.168.2.5216.218.135.1184971994972816766 02/02/23-13:54:17.287135
SID:	2816766

Source Port:	49719
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	−
Timestamp:	192.168.2.5216.218.135.1184970794972025019 02/02/23-13:53:11.027058
SID:	2025019
Source Port:	49707
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	−
Timestamp:	192.168.2.5216.218.135.1184970694972816766 02/02/23-13:53:06.659044
SID:	2816766
Source Port:	49706
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	−
Timestamp:	192.168.2.5216.218.135.1184971694972816766 02/02/23-13:53:51.482545
SID:	2816766
Source Port:	49716
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	−
Timestamp:	192.168.2.5216.218.135.1184971894972816766 02/02/23-13:54:10.762374
SID:	2816766
Source Port:	49718
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	−
Timestamp:	192.168.2.5216.218.135.1184971394972816718 02/02/23-13:53:38.638029
SID:	2816718
Source Port:	49713
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	−
Timestamp:	192.168.2.5216.218.135.1184970594972816766 02/02/23-13:52:47.006733
SID:	2816766
Source Port:	49705
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	−
Timestamp:	192.168.2.5216.218.135.1184971694972025019 02/02/23-13:53:49.540253
SID:	2025019
Source Port:	49716
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184970694972025019 02/02/23-13:53:04.914468
SID:	2025019
Source Port:	49706
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184970994972816766 02/02/23-13:53:19.141097
SID:	2816766
Source Port:	49709
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184971994972025019 02/02/23-13:54:15.331062
SID:	2025019
Source Port:	49719
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184970494972816766 02/02/23-13:52:39.164512
SID:	2816766
Source Port:	49704
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184970394972025019 02/02/23-13:52:31.077436
SID:	2025019
Source Port:	49703
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184970994972025019 02/02/23-13:53:17.202283
SID:	2025019
Source Port:	49709
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184972094972816766 02/02/23-13:54:23.957947
SID:	2816766
Source Port:	49720
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	
Timestamp:	192.168.2.5216.218.135.1184970594972025019 02/02/23-13:52:43.940467
SID:	2025019
Source Port:	49705

Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	▬
Timestamp:	192.168.2.5216.218.135.1184971494972816766 02/02/23-13:53:44.997752
SID:	2816766
Source Port:	49714
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	▬
Timestamp:	192.168.2.5216.218.135.1184971394972025019 02/02/23-13:53:36.615923
SID:	2025019
Source Port:	49713
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	▬
Timestamp:	192.168.2.5216.218.135.1184970394972816766 02/02/23-13:52:32.924340
SID:	2816766
Source Port:	49703
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	▬
Timestamp:	192.168.2.5216.218.135.1184971894972025019 02/02/23-13:54:08.817214
SID:	2025019
Source Port:	49718
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	▬
Timestamp:	192.168.2.5216.218.135.1184972094972025019 02/02/23-13:54:21.603489
SID:	2025019
Source Port:	49720
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	▬
Timestamp:	192.168.2.5216.218.135.1184970794972816766 02/02/23-13:53:12.773010
SID:	2816766
Source Port:	49707
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 216.218.135.118	▬
Timestamp:	192.168.2.5216.218.135.1184971394972816766 02/02/23-13:53:38.843314
SID:	2816766
Source Port:	49713
Destination Port:	9497
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

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)

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

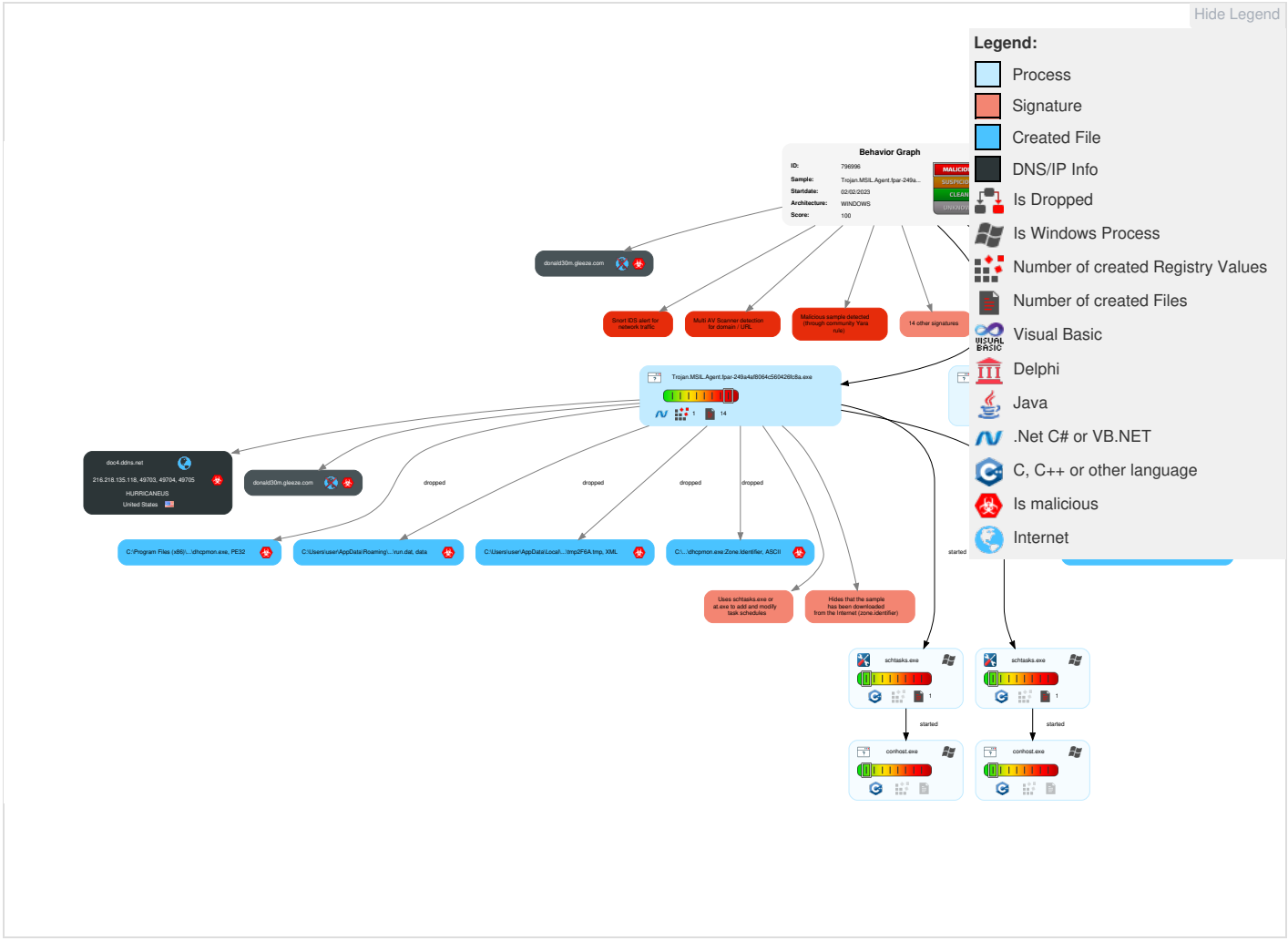
Detected Nanocore Rat

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	1 Scheduled Task/Job	1 Scheduled Task/Job	1 Access Token Manipulation	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 2 Process Injection	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)	1 Scheduled Task/Job	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)	1 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 Process Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

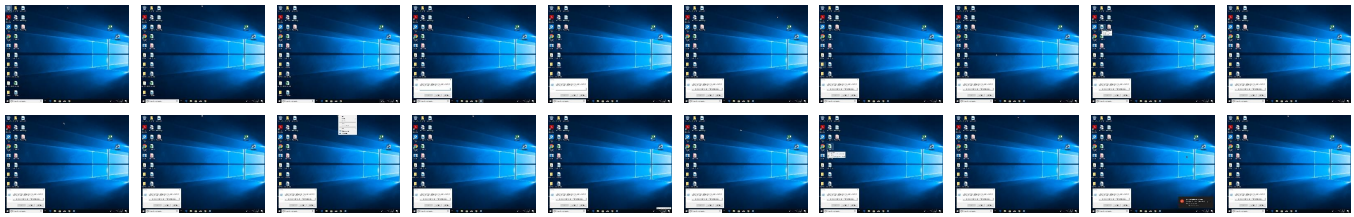
Behavior Graph



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
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	77%	Virustotal		Browse
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	100%	Avira	TR/Dropper.Gen	
Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.Gen	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.2f0000.0.unpack	100%	Avira	HEUR/AGEN.1208316		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.55c0000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
doc4.ddns.net	9%	Virustotal		Browse
donald30m.gleeze.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
doc4.ddns.net	100%	Avira URL Cloud	malware	
donald30m.gleeze.com	100%	Avira URL Cloud	malware	
doc4.ddns.net	9%	Virustotal		Browse

Domains and IPs

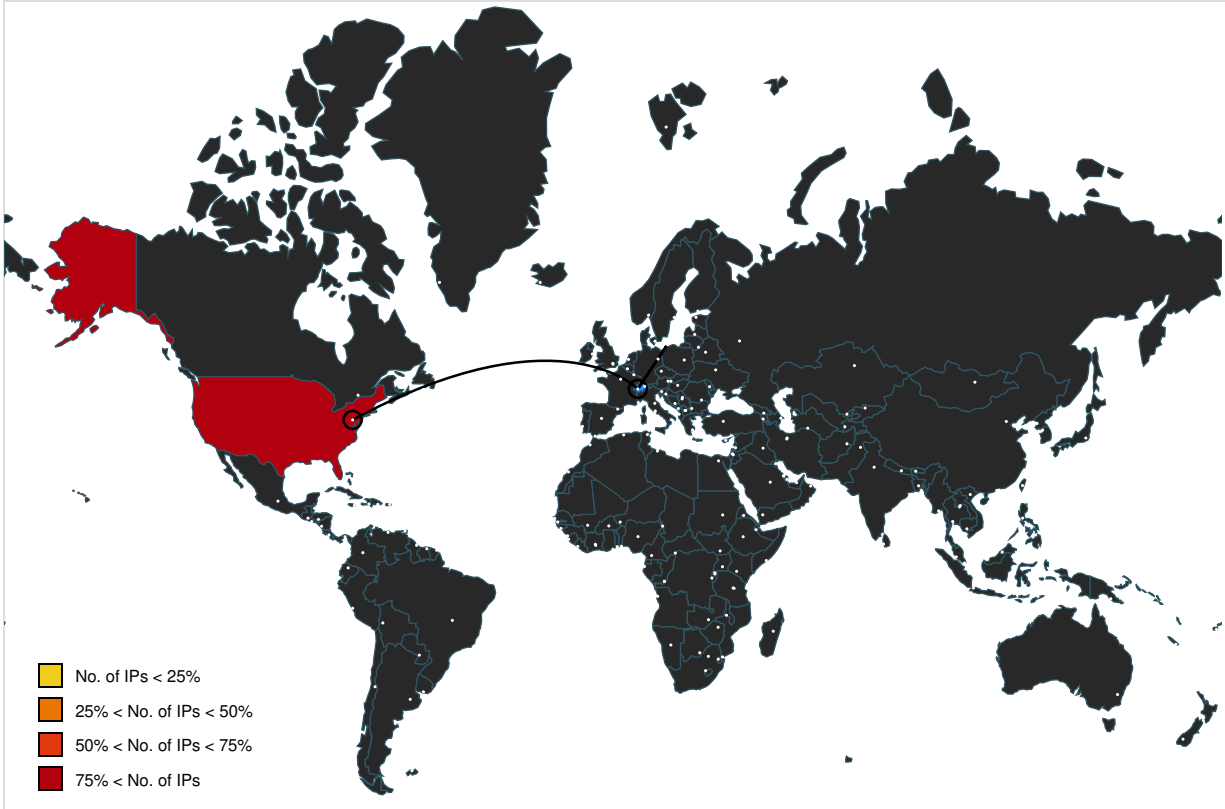
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
doc4.ddns.net	216.218.135.118	true	true	• 9%, Virustotal, Browse	unknown
donald30m.gleeze.com	unknown	unknown	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
doc4.ddns.net	true	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown
donald30m.gleeze.com	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.218.135.118	doc4.ddns.net	United States		6939	HURRICANEUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796996
Start date and time:	2023-02-02 13:51:27 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
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
Sample file name:	Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/8@45/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- 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.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:52:29	API Interceptor	899x Sleep call for process: Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe modified
13:52:31	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe" s>$(Arg0)
13:52:31	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
13:52:32	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:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	208192
Entropy (8bit):	7.452519436311911
Encrypted:	false
SSDEEP:	6144:nLV6Bta6dtJmakIM57s7UBmOKqVotp/wK328:nLV6BtpmkBQmGuAK328
MD5:	E587236CB6E5CCF2497AB08B245F724F
SHA1:	8B9F158FD574C4E982EC73E2368EBB4F6E4B566B
SHA-256:	249A4AF8064C560426FC8AEA6FC23EE47A24BA800628D805F9EB0653B8E1D4F9
SHA-512:	79BDF02544E533312D2BD9D5D899690A59E2713F6958210E30B8A41699B7752EE8EE939C4FCACFC5E57A1E22BE21F228BFDEC5990D24C1D23D403F65383B0CA D
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Reputation:	low
Preview:	MZ.....@.....m..:.^r.V.is program cannot be run in DOS mode....$.....PE..L...u9^..x8.....b..... .....@.. ....8...W.... ..._..... ....H.....text..... ....`.reloc.....@..B.elo....._... . ..`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....- (&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0. .$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

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

Process:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.log

Process:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.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
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp2F6A.tmp

Process:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	5.155039726320282
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PuL+mGIaxtn:cbk4oL600QydbQxIYODOLedq3S88j
MD5:	48F81422D81C15F6FEB04712FA462929
SHA1:	54B98A94C873D79855E2806FCE3BF7595BDDAB36
SHA-256:	77322090BB966A60FB35A96818844E8EEC195EDE49506403FD30D13315CF384E
SHA-512:	28F72799A3867282529E38141BC4FB454C6843D3DC8DED4D9384A7B186A7B9E54F83D28DDF95EF92D92D6E51AB687A928BFD7A3641E0BF353B48BFC4A6D92A5D
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp315F.tmp

Process:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:eQh7t:eQZt
MD5:	3CBD21D820A416CE1F45D62B147FA3CD
SHA1:	51CDCBD1B4B1483FAD4341D6FA7344F7012A7E5D
SHA-256:	1998F131D77CE0373D863042818B8A524A2A8336C8CB089D80287402E7A42B47
SHA-512:	FDEF9C4C21C8B53BAC3EA192C0EB48786EC39EABFC3105F87C735B0F07D6124B52EB710652AF5E2A1F8393928D760644018FB4D7E78BA2A3AEAD769FB0823323
Malicious:	**true**
Preview:	.n5.g..H

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

Process:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	73
Entropy (8bit):	4.84545516864142
Encrypted:	false
SSDEEP:	3:oNUWJRWxXUELLo22q+qgTRGGfWjC:oNNJAuEgJq+HGGfWjC
MD5:	1651BC143CC1BD2E5044B75929ED5180
SHA1:	893475F94E765C92D08821CEBD0F72181884B8C7
SHA-256:	34D493A6599BE5BF5CBFCCEA666D545AD33D9A85556ACA4E1219FEACB38D14A1
SHA-512:	2355872BF1572ABB70FFB53076DC746D86300006832B9B2837420F5A74AC0732CCD10C1F72AC67F3245367FDA49E4C0561DA46F5DC55FCB7D33B8AF1057F19F
Malicious:	false
Preview:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.452519436311911
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
File size:	208192
MD5:	e587236cb6e5ccf2497ab08b245f724f
SHA1:	8b9f158fd574c4e982ec73e2368ebb4f6e4b566b
SHA256:	249a4af8064c560426fc8aea6fc23ee47a24ba800628d805f9eb0653b8e1d4f9
SHA512:	79bdf02544e533312d2bd9d5d899690a59e2713f6958210e30b8a41699b7752ee8ee939c4fcacfc5e57a1e22be21f228bfdec5990d24c1d23d403f65383b0cad
SSDEEP:	6144:nLV6Bta6dtJmakIM57s7UBmOKqVotp/wK328:nLV6BtpmkBQmGuAK328
TLSH:	3014CF2677A84A2FE2DE86BD702251168379C2E398C3F7DE28D451B78F167E10A471D3
File Content Preview:	MZ.....@.....m..:.^r.V.is program cannot be run in DOS mode....$.....PE..L...u9^..x8.....b..... .....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA
Time Stamp:	0x9E5E3975 [Fri Mar 13 00:40:21 2054 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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 dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add cl, ah
xor dword ptr [esi-24h], FFFFFFD7h
push edx
sub dword ptr [ecx], ecx
pop edi
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
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	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x15fd8	.elo
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	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	0x1c800	0x1c800	False	0.5946494654605263	data	6.598686715608938	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0x200	0x200	False	0.076171875	data	0.32171607431271465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.elo	0x22000	0x15fd8	0x16000	False	1.0003107244318181	data	7.9978558519507255	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x15f80	data		

Imports	
DLL	**Import**
mscoree.dll	_CorExeMain

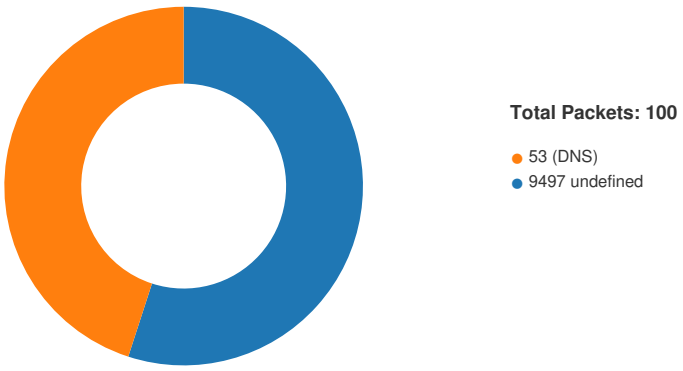
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5216.218.135.118497049497202501902/02/23-13:52:37.416548	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497149497202501902/02/23-13:53:43.248786	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497049497281671802/02/23-13:52:37.610379	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49704	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497199497281676602/02/23-13:54:17.287135	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497079497202501902/02/23-13:53:11.027058	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497069497281676602/02/23-13:53:06.659044	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497169497281676602/02/23-13:53:51.482545	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497189497281676602/02/23-13:54:10.762374	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497139497281671802/02/23-13:53:38.638029	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49713	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497059497281676602/02/23-13:52:47.006733	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497169497202501902/02/23-13:53:49.540253	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497069497202501902/02/23-13:53:04.914468	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497099497281676602/02/23-13:53:19.141097	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497199497202501902/02/23-13:54:15.331062	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.118497049497281676602/02/23-13:52:39.164512	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	9497	192.168.2.5	216.218.135.118

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5216.218.135.1184970394972025019 02/02/23-13:52:31.077436	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184970994972025019 02/02/23-13:53:17.202283	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184972094972816766 02/02/23-13:54:23.957947	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184970594972025019 02/02/23-13:52:43.940467	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184971494972816766 02/02/23-13:53:44.997752	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184971394972025019 02/02/23-13:53:36.615923	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184970394972816766 02/02/23-13:52:32.924340	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184971894972025019 02/02/23-13:54:08.817214	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184972094972025019 02/02/23-13:54:21.603489	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184970794972816766 02/02/23-13:53:12.773010	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	9497	192.168.2.5	216.218.135.118
192.168.2.5216.218.135.1184971394972816766 02/02/23-13:53:38.843314	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	9497	192.168.2.5	216.218.135.118

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 13:52:30.829849005 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:31.024633884 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:31.024909019 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:31.077435970 CET	49703	9497	192.168.2.5	216.218.135.118

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 13:52:31.271203995 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:31.368933916 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:31.565625906 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:31.565787077 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:31.759715080 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:31.759888887 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:31.953443050 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:31.953566074 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:32.149359941 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:32.149508953 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:32.343123913 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:32.343324900 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:32.536889076 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:32.536986113 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:32.730629921 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:32.730711937 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:32.924274921 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:32.924340010 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:33.032847881 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:33.117907047 CET	9497	49703	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:33.117973089 CET	49703	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:37.220767975 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:37.415462971 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:37.415747881 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:37.416548014 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:37.610068083 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:37.610378981 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:37.804006100 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:37.804152012 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:37.997829914 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:37.997968912 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:38.191600084 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:38.191828012 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:38.386626959 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:38.386846066 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:38.580442905 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:38.580596924 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:38.776628017 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:38.776709080 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:38.970408916 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:38.970501900 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:39.164345026 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:39.164511919 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:39.269047976 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:39.358289003 CET	9497	49704	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:39.358375072 CET	49704	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:43.746020079 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:43.939932108 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:43.940032005 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:43.940466881 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:44.134073019 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:44.134223938 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:44.328047037 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:44.918446064 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:45.112292051 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:45.454889059 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:45.648586988 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:45.648741007 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:45.843472958 CET	9497	49705	216.218.135.118	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 13:52:45.843571901 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:46.037422895 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:46.037647009 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:46.231372118 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:46.231483936 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:46.425019979 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:46.425132990 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:46.618844986 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:46.619046926 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:46.812693119 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:46.812881947 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:47.006531954 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:47.006732941 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:47.017621994 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:52:47.200439930 CET	9497	49705	216.218.135.118	192.168.2.5
Feb 2, 2023 13:52:47.200515985 CET	49705	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:04.719393969 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:04.913069963 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:04.913290977 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:04.914468050 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:05.108067989 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:05.108247995 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:05.301942110 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:05.302042961 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:05.495675087 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:05.495810986 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:05.689413071 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:05.689577103 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:05.883318901 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:05.883480072 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:06.077214956 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:06.077378035 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:06.271008015 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:06.271168947 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:06.465250015 CET	9497	49706	216.218.135.118	192.168.2.5
Feb 2, 2023 13:53:06.465341091 CET	49706	9497	192.168.2.5	216.218.135.118
Feb 2, 2023 13:53:06.658847094 CET	9497	49706	216.218.135.118	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 13:52:30.785638094 CET	49177	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:52:30.809514999 CET	53	49177	8.8.8.8	192.168.2.5
Feb 2, 2023 13:52:37.192082882 CET	49724	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:52:37.213845968 CET	53	49724	8.8.8.8	192.168.2.5
Feb 2, 2023 13:52:43.715668917 CET	61452	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:52:43.735198975 CET	53	61452	8.8.8.8	192.168.2.5
Feb 2, 2023 13:52:51.099303961 CET	65323	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:52:51.274023056 CET	53	65323	8.8.8.8	192.168.2.5
Feb 2, 2023 13:52:51.381551981 CET	51484	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:52:51.401228905 CET	53	51484	8.8.4.4	192.168.2.5
Feb 2, 2023 13:52:51.439233065 CET	63446	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:52:51.609329939 CET	53	63446	8.8.8.8	192.168.2.5
Feb 2, 2023 13:52:55.884648085 CET	56751	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:52:56.024313927 CET	53	56751	8.8.8.8	192.168.2.5
Feb 2, 2023 13:52:56.089971066 CET	55039	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:52:56.109600067 CET	53	55039	8.8.4.4	192.168.2.5
Feb 2, 2023 13:52:56.136313915 CET	60975	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:52:56.309134007 CET	53	60975	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 13:53:00.369370937 CET	59220	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:00.388981104 CET	53	59220	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:00.394347906 CET	55068	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:53:00.413863897 CET	53	55068	8.8.4.4	192.168.2.5
Feb 2, 2023 13:53:00.573218107 CET	56682	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:00.590332985 CET	53	56682	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:04.664993048 CET	58532	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:04.685724974 CET	53	58532	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:10.799266100 CET	62659	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:10.820059061 CET	53	62659	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:16.983659983 CET	56263	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:17.001274109 CET	53	56263	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:23.341100931 CET	64419	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:23.513459921 CET	53	64419	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:23.532455921 CET	52688	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:53:23.550225019 CET	53	52688	8.8.4.4	192.168.2.5
Feb 2, 2023 13:53:23.554807901 CET	61344	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:23.576509953 CET	53	61344	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:27.656083107 CET	53972	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:27.675067902 CET	53	53972	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:27.676650047 CET	64932	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:53:27.847728014 CET	53	64932	8.8.4.4	192.168.2.5
Feb 2, 2023 13:53:27.935981035 CET	58472	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:27.953819990 CET	53	58472	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:31.993725061 CET	60284	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:32.013403893 CET	53	60284	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:32.015000105 CET	60019	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:53:32.032545090 CET	53	60019	8.8.4.4	192.168.2.5
Feb 2, 2023 13:53:32.056422949 CET	50902	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:32.075882912 CET	53	50902	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:36.397737026 CET	53823	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:36.415522099 CET	53	53823	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:43.025010109 CET	49769	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:43.046535015 CET	53	49769	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:49.326673031 CET	53555	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:49.344393969 CET	53	53555	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:55.632159948 CET	61293	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:55.652245998 CET	53	61293	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:55.654360056 CET	50086	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:53:55.673933983 CET	53	50086	8.8.4.4	192.168.2.5
Feb 2, 2023 13:53:55.682020903 CET	52188	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:55.701627016 CET	53	52188	8.8.8.8	192.168.2.5
Feb 2, 2023 13:53:59.949156046 CET	54585	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:53:59.966969967 CET	53	54585	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:00.025202990 CET	52100	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:54:00.045074940 CET	53	52100	8.8.4.4	192.168.2.5
Feb 2, 2023 13:54:00.234499931 CET	60908	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:00.253770113 CET	53	60908	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:04.278805017 CET	58623	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:04.296454906 CET	53	58623	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:04.298249006 CET	65493	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:54:04.317616940 CET	53	65493	8.8.4.4	192.168.2.5
Feb 2, 2023 13:54:04.329217911 CET	57482	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:04.349050999 CET	53	57482	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:08.551012039 CET	62057	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:08.570725918 CET	53	62057	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:15.050424099 CET	60294	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:15.067796946 CET	53	60294	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:21.385283947 CET	63728	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 13:54:21.405025959 CET	53	63728	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:29.207783937 CET	50077	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:29.229578018 CET	53	50077	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:29.422302008 CET	49959	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:54:29.441528082 CET	53	49959	8.8.4.4	192.168.2.5
Feb 2, 2023 13:54:29.449975014 CET	55609	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:29.470909119 CET	53	55609	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:37.122015953 CET	52892	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:37.139646053 CET	53	52892	8.8.8.8	192.168.2.5
Feb 2, 2023 13:54:37.141393900 CET	65330	53	192.168.2.5	8.8.4.4
Feb 2, 2023 13:54:37.159055948 CET	53	65330	8.8.4.4	192.168.2.5
Feb 2, 2023 13:54:37.165865898 CET	52973	53	192.168.2.5	8.8.8.8
Feb 2, 2023 13:54:37.184803963 CET	53	52973	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 2, 2023 13:52:30.785638094 CET	192.168.2.5	8.8.8.8	0x84a	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:37.192082882 CET	192.168.2.5	8.8.8.8	0x1c22	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:43.715668917 CET	192.168.2.5	8.8.8.8	0x33de	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:51.099303961 CET	192.168.2.5	8.8.8.8	0xd6f6	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:51.381551981 CET	192.168.2.5	8.8.4.4	0xb8b0	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:51.439233065 CET	192.168.2.5	8.8.8.8	0xe20e	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:55.884648085 CET	192.168.2.5	8.8.8.8	0x81a3	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:56.089971066 CET	192.168.2.5	8.8.4.4	0x4ccf	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:56.136313915 CET	192.168.2.5	8.8.8.8	0xf4e4	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:00.369370937 CET	192.168.2.5	8.8.8.8	0x44a0	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:00.394347906 CET	192.168.2.5	8.8.4.4	0x83b4	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:00.573218107 CET	192.168.2.5	8.8.8.8	0x9279	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:04.664993048 CET	192.168.2.5	8.8.8.8	0xd0ac	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:10.799266100 CET	192.168.2.5	8.8.8.8	0xf1a6	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:16.983659983 CET	192.168.2.5	8.8.8.8	0x83b9	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:23.341100931 CET	192.168.2.5	8.8.8.8	0x9df6	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:23.532455921 CET	192.168.2.5	8.8.4.4	0x3466	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:23.554807901 CET	192.168.2.5	8.8.8.8	0x6152	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:27.656083107 CET	192.168.2.5	8.8.8.8	0x626d	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:27.676650047 CET	192.168.2.5	8.8.4.4	0xbe1b	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:27.935981035 CET	192.168.2.5	8.8.8.8	0x9dc2	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:31.993725061 CET	192.168.2.5	8.8.8.8	0x6900	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:32.015000105 CET	192.168.2.5	8.8.4.4	0x2c34	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:32.056422949 CET	192.168.2.5	8.8.8.8	0x70ec	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:36.397737026 CET	192.168.2.5	8.8.8.8	0x7750	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 2, 2023 13:53:43.025010109 CET	192.168.2.5	8.8.8.8	0x1c56	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:49.326673031 CET	192.168.2.5	8.8.8.8	0x139b	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:55.632159948 CET	192.168.2.5	8.8.8.8	0x77fd	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:55.654360056 CET	192.168.2.5	8.8.4.4	0x4540	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:55.682020903 CET	192.168.2.5	8.8.8.8	0x1461	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:59.949156046 CET	192.168.2.5	8.8.8.8	0xe785	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:00.025202990 CET	192.168.2.5	8.8.4.4	0x1f2	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:00.234499931 CET	192.168.2.5	8.8.8.8	0x434d	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:04.278805017 CET	192.168.2.5	8.8.8.8	0xb31e	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:04.298249006 CET	192.168.2.5	8.8.4.4	0x7ccc	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:04.329217911 CET	192.168.2.5	8.8.8.8	0xa5b5	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:08.551012039 CET	192.168.2.5	8.8.8.8	0x2481	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:15.050424099 CET	192.168.2.5	8.8.8.8	0x4a5c	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:21.385283947 CET	192.168.2.5	8.8.8.8	0x9ec8	Standard query (0)	doc4.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:29.207783937 CET	192.168.2.5	8.8.8.8	0x40b9	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:29.422302008 CET	192.168.2.5	8.8.4.4	0xe659	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:29.449975014 CET	192.168.2.5	8.8.8.8	0x4fee	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:37.122015953 CET	192.168.2.5	8.8.8.8	0xde39	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:37.141393900 CET	192.168.2.5	8.8.4.4	0xeb1a	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:37.165865898 CET	192.168.2.5	8.8.8.8	0x6dc4	Standard query (0)	donald30m.gleeze.com	A (IP address)	IN (0x0001)	false

DNS Answers

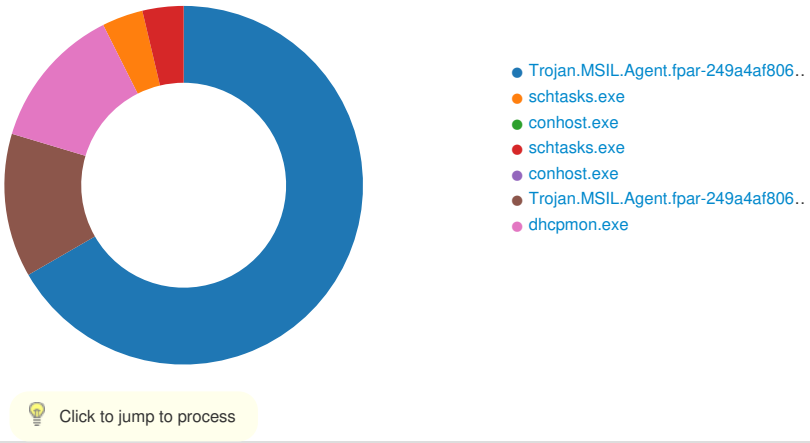
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2023 13:52:30.809514999 CET	8.8.8.8	192.168.2.5	0x84a	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:37.213845968 CET	8.8.8.8	192.168.2.5	0x1c22	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:43.735198975 CET	8.8.8.8	192.168.2.5	0x33de	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:51.274023056 CET	8.8.8.8	192.168.2.5	0xd6f6	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:51.401228905 CET	8.8.4.4	192.168.2.5	0xb8b0	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:51.609329939 CET	8.8.8.8	192.168.2.5	0xe20e	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:56.024313927 CET	8.8.8.8	192.168.2.5	0x81a3	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:56.109600067 CET	8.8.4.4	192.168.2.5	0x4ccf	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:52:56.309134007 CET	8.8.8.8	192.168.2.5	0xf4e4	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2023 13:53:00.388981104 CET	8.8.8.8	192.168.2.5	0x44a0	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:00.413863897 CET	8.8.4.4	192.168.2.5	0x83b4	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:00.590332985 CET	8.8.8.8	192.168.2.5	0x9279	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:04.685724974 CET	8.8.8.8	192.168.2.5	0xd0ac	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:10.820059061 CET	8.8.8.8	192.168.2.5	0xf1a6	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:17.001274109 CET	8.8.8.8	192.168.2.5	0x83b9	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:23.513459921 CET	8.8.8.8	192.168.2.5	0x9df6	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:23.550225019 CET	8.8.4.4	192.168.2.5	0x3466	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:23.576509953 CET	8.8.8.8	192.168.2.5	0x6152	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:27.675067902 CET	8.8.8.8	192.168.2.5	0x626d	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:27.847728014 CET	8.8.4.4	192.168.2.5	0xbe1b	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:27.953819990 CET	8.8.8.8	192.168.2.5	0x9dc2	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:32.013403893 CET	8.8.8.8	192.168.2.5	0x6900	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:32.032545090 CET	8.8.4.4	192.168.2.5	0x2c34	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:32.075882912 CET	8.8.8.8	192.168.2.5	0x70ec	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:36.415522099 CET	8.8.8.8	192.168.2.5	0x7750	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:43.046535015 CET	8.8.8.8	192.168.2.5	0x1c56	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:49.344393969 CET	8.8.8.8	192.168.2.5	0x139b	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:55.652245998 CET	8.8.8.8	192.168.2.5	0x77fd	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:55.673933983 CET	8.8.4.4	192.168.2.5	0x4540	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:55.701627016 CET	8.8.8.8	192.168.2.5	0x1461	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:53:59.966969967 CET	8.8.8.8	192.168.2.5	0xe785	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:00.045074940 CET	8.8.4.4	192.168.2.5	0x1f2	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:00.253770113 CET	8.8.8.8	192.168.2.5	0x434d	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:04.296454906 CET	8.8.8.8	192.168.2.5	0xb31e	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2023 13:54:04.317616940 CET	8.8.4.4	192.168.2.5	0x7ccc	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:04.349050999 CET	8.8.8.8	192.168.2.5	0xa5b5	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:08.570725918 CET	8.8.8.8	192.168.2.5	0x2481	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:15.067796946 CET	8.8.8.8	192.168.2.5	0x4a5c	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:21.405025959 CET	8.8.8.8	192.168.2.5	0x9ec8	No error (0)	doc4.ddns.net		216.218.135.118	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:29.229578018 CET	8.8.8.8	192.168.2.5	0x40b9	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:29.441528082 CET	8.8.4.4	192.168.2.5	0xe659	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:29.470909119 CET	8.8.8.8	192.168.2.5	0x4fee	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:37.139646053 CET	8.8.8.8	192.168.2.5	0xde39	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:37.159055948 CET	8.8.4.4	192.168.2.5	0xeb1a	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false
Feb 2, 2023 13:54:37.184803963 CET	8.8.8.8	192.168.2.5	0x6dc4	Name error (3)	donald30m.gleeze.com	none	none	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe PID: **5044**, Parent PID: **3324**

General

Target ID:	0
Start time:	13:52:27

Start date:	02/02/2023
Path:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
Imagebase:	0x2f0000
File size:	208192 bytes
MD5 hash:	E587236CB6E5CCF2497AB08B245F724F
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: 00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000000.309491180.00000000002F2000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.584551400.00000000055C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.584551400.00000000055C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.584551400.00000000055C0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.584551400.00000000055C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.584551400.00000000055C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.584012735.0000000004CA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.584012735.0000000004CA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.584012735.0000000004CA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.584012735.0000000004CA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.579767237.00000000029B1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6BF460AC	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	6BF460AC	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	2630D15	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	2630E0F	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	2630D15	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	2631094	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2631094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2F6A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2631290	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	2630E0F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp315F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2631290	GetTempFileNameW
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	2630D15	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	2630D15	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	6BF460AC	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	6BF460AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2F6A.tmp	success or wait	1	6B527D95	unknown
C:\Users\user\AppData\Local\Temp\tmp315F.tmp	success or wait	1	6B527D95	unknown
C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe:Zone.Identifier	success or wait	1	2631625	DeleteFileA

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 6e 35 fd 67 05 fd 48	n5gH	success or wait	1	2630FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 02 00 fd 00 00 00 02 00 00 00 40 00 02 00 00 00 00 00 00 00 00 00 08 00 04 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 6d fd fd 3a fd 5e 72 fd 56 fd 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 75 39 5e fd fd 78 38 fd f4 fd fd fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 62 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 20 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@m:^rVis program cannot be run in DOS mode.$PELu9^x8b @	success or wait	2	2631094	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	2631094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2F6A.tmp	0	1336	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	2630FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	73	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 54 72 6f 6a 61 6e 2e 4d 53 49 4c 2e 41 67 65 6e 74 2e 66 70 61 72 2d 32 34 39 61 34 61 66 38 30 36 34 63 35 36 30 34 32 36 66 63 38 61 2e 65 78 65	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	success or wait	1	2630FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp315F.tmp	0	1310	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	2630FC7	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	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BF78738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6C01BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6C01BF06	unknown
C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	unknown	4096	success or wait	1	6C01BF06	unknown
C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe	unknown	512	success or wait	1	6C01BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2630FC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6C01BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6C01BF06	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	2631186	RegSetValueExW

Analysis Process: schtasks.exe PID: **2472**, Parent PID: **5044**

General

Target ID:	1

Start time:	13:52:28
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp2F6A.tmp
Imagebase:	0x1280000
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\tmp2F6A.tmp	unknown	2	success or wait	1	128AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2F6A.tmp	unknown	1337	success or wait	1	128ABD9	ReadFile

Analysis Process: conhost.exe PID: **4956**, Parent PID: **2472**

General

Target ID:	2
Start time:	13:52:28
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: schtasks.exe PID: **4852**, Parent PID: **5044**

General

Target ID:	3
Start time:	13:52:29
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp315F.tmp
Imagebase:	0x1280000
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\tmp315F.tmp	unknown	2	success or wait	1	128AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp315F.tmp	unknown	1311	success or wait	1	128ABD9	ReadFile

Analysis Process: conhost.exe PID: **4964**, Parent PID: **4852**

General

Target ID:	4
Start time:	13:52:29
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe PID: **1244**, Parent PID: **1084**

General

Target ID:	5
Start time:	13:52:31
Start date:	02/02/2023
Path:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe 0
Imagebase:	0x4d0000
File size:	208192 bytes
MD5 hash:	E587236CB6E5CCF2497AB08B245F724F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.333232507.0000000002AD1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.333232507.0000000002AD1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000002.333232507.0000000002AD1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6BF460AC	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	6BF460AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF334A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Trojan.MSIL.Agent.fpar-249a4af8064c560426fc8a.exe.log	0	525	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 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6C21A33A	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	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BF78738	ReadFile

Analysis Process: dhcpmon.exe PID: **2148**, Parent PID: **1084**

General

Target ID:	6
Start time:	13:52:31
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xcb0000
File size:	208192 bytes
MD5 hash:	E587236CB6E5CCF2497AB08B245F724F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.333152349.0000000004461000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.333152349.0000000004461000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.333152349.0000000004461000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.332991768.0000000003461000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.332991768.0000000003461000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.332991768.0000000003461000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 97%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BF460AC	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	6BF460AC	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	6BF334A7	CreateFileW

File Written

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	0	525	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 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6C21A33A	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	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6BF75544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BF78738	ReadFile

Disassembly

No disassembly