ID: 384377
Sample Name: nanocore.exe
Cookbook: default.jbs
Time: 01:07:10
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

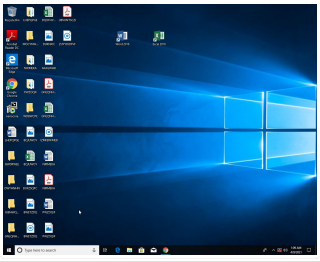
Analysis Report nanocore.exe

Overview

General Information

Sample Name:	nanocore.exe
Analysis ID:	384377
MD5:	08803cc817d8b1..
SHA1:	8d76cc9e4e21f90..
SHA256:	00343ef156007c4..
Tags:	Nanocore
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

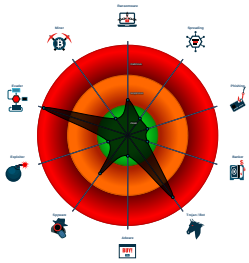
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loc…

Classification



Startup

- **System is w10x64**
- nanocore.exe (PID: 7064 cmdline: 'C:\Users\user\Desktop\nanocore.exe' MD5: 08803CC817D8B1046A964AF11685B15C)
  - nanocore.exe (PID: 7104 cmdline: 'C:\Users\user\Desktop\nanocore.exe' MD5: 08803CC817D8B1046A964AF11685B15C)
    - schtasks.exe (PID: 5800 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp38C1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5108 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp3B81.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nanocore.exe (PID: 4108 cmdline: C:\Users\user\Desktop\nanocore.exe 0 MD5: 08803CC817D8B1046A964AF11685B15C)
  - nanocore.exe (PID: 5904 cmdline: C:\Users\user\Desktop\nanocore.exe 0 MD5: 08803CC817D8B1046A964AF11685B15C)
- dhcpmon.exe (PID: 5752 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 08803CC817D8B1046A964AF11685B15C)
  - dhcpmon.exe (PID: 6152 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 08803CC817D8B1046A964AF11685B15C)
- dhcpmon.exe (PID: 6724 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 08803CC817D8B1046A964AF11685B15C)
  - dhcpmon.exe (PID: 6704 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 08803CC817D8B1046A964AF11685B15C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "bee718f3-e47a-44f8-955e-2fe2c6c0",
  "Group": "Default",
  "Domain1": "chinomso.duckdns.org",
  "Domain2": "chinomso.duckdns.org",
  "Port": 7688,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "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": "chinomso.duckdns.org",
  "BackupDNSServer": "chinomso.duckdns.orgAMC9Avo9uFWUE1JbxpU=",
  "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 Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2135d:$x1: NanoCore Client.exe • 0x215e5:$x2: NanoCore.ClientPluginHost • 0x22c1e:$s1: PluginCommand • 0x22c12:$s2: FileCommand • 0x23ac3:$s3: PipeExists • 0x2987a:$s4: PipeCreated • 0x2160f:$s5: IClientLoggingHost
00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2134d:$a: NanoCore • 0x2135d:$a: NanoCore • 0x21591:$a: NanoCore • 0x215a5:$a: NanoCore • 0x215e5:$a: NanoCore • 0x213ac:$b: ClientPlugin • 0x215ae:$b: ClientPlugin • 0x215ee:$b: ClientPlugin • 0x214d3:$c: ProjectData • 0x21eda:$d: DESCrypto • 0x298a6:$e: KeepAlive • 0x27894:$g: LogClientMessage • 0x23a8f:$i: get_Connected • 0x22210:$j: #=q • 0x22240:$j: #=q • 0x2225c:$j: #=q • 0x2228c:$j: #=q • 0x222a8:$j: #=q • 0x222c4:$j: #=q • 0x222f4:$j: #=q • 0x22310:$j: #=q

Source	Rule	Description	Author	Strings
0000000A.00000002.683529518.000000000067 9000.00000004.00000020.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2db9d:$x1: NanoCore.ClientPluginHost • 0x2dbda:$x2: IClientNetworkHost • 0x3170d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 132 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.1.nanocore.exe.415058.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
10.1.nanocore.exe.415058.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
10.1.nanocore.exe.415058.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
10.1.nanocore.exe.415058.1.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
11.2.dhcpmon.exe.415058.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 352 entries				

Sigma Overview

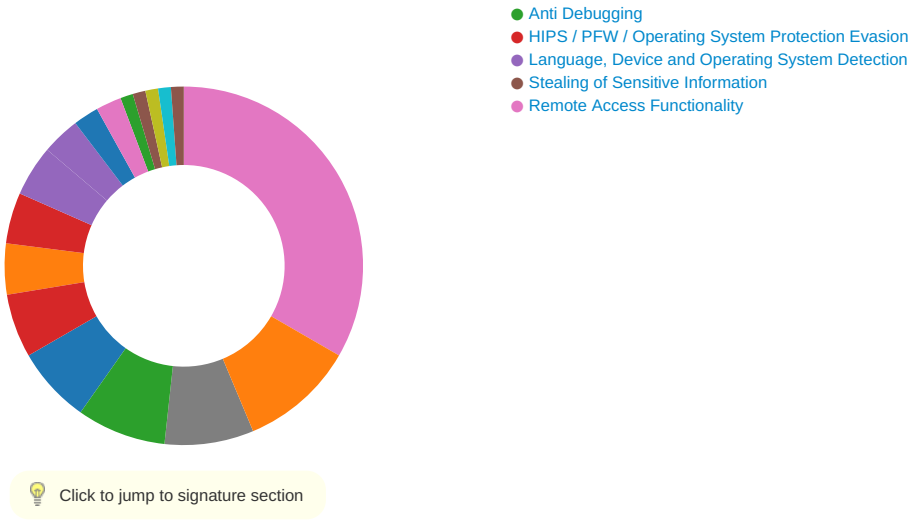
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion



AV Detection:

- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT

Compliance:

- Detected unpacking (creates a PE file in dynamic memory)
- Detected unpacking (overwrites its own PE header)

Networking:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (creates a PE file in dynamic memory)
- Detected unpacking (overwrites its own PE header)
- .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)

HIPS / PFW / Operating System Protection Evasion:

Contains functionality to prevent local Windows debugging

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

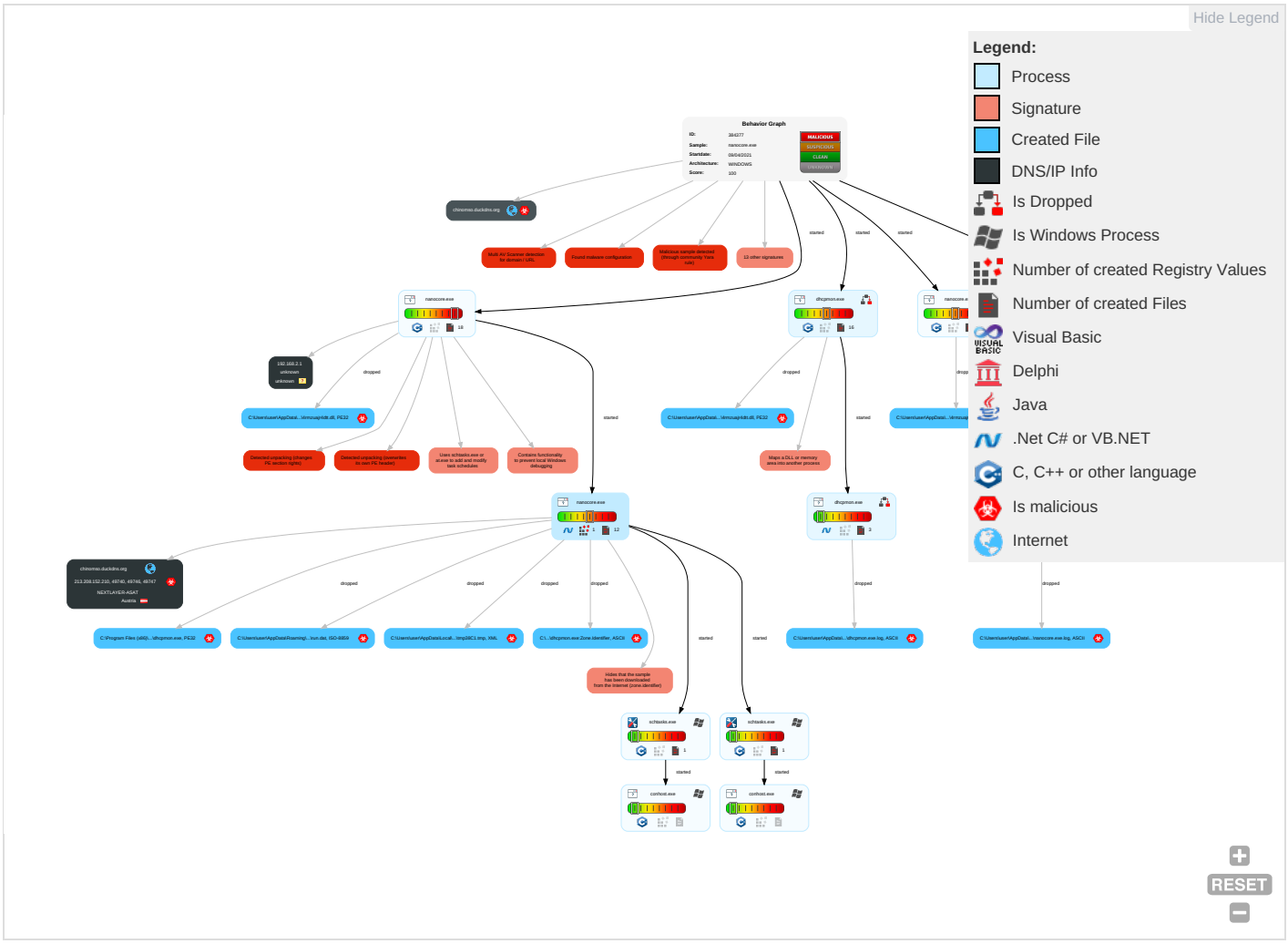
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Scheduled Task/Job 1	Process Injection 2 1 2	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 2 4	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 4 1	NTDS	Security Software Discovery 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

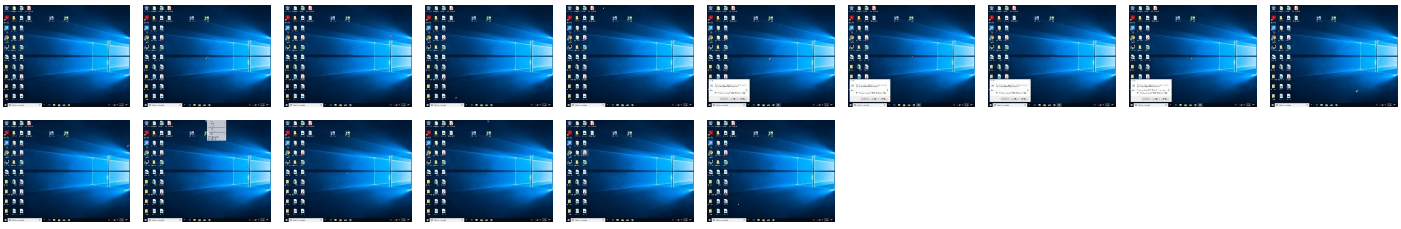
Behavior Graph



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
nanocore.exe	21%	Virustotal		Browse
nanocore.exe	34%	ReversingLabs	Win32.Trojan.Predator	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	34%	ReversingLabs	Win32.Trojan.Predator	
C:\Users\user\AppData\Local\Temp\nse444B.tmp\4rmzuajr4dtt.dll	24%	ReversingLabs	Win32.Trojan.Predator	
C:\Users\user\AppData\Local\Temp\nsj42E4.tmp\4rmzuajr4dtt.dll	24%	ReversingLabs	Win32.Trojan.Predator	
C:\Users\user\AppData\Local\Temp\nsn2692.tmp\4rmzuajr4dtt.dll	24%	ReversingLabs	Win32.Trojan.Predator	
C:\Users\user\AppData\Local\Temp\nsq6D11.tmp\4rmzuajr4dtt.dll	24%	ReversingLabs	Win32.Trojan.Predator	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.dhcpmon.exe.4920000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.nanocore.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.nanocore.exe.49c0000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.nanocore.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.nanocore.exe.4a90000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
13.2.dhcpmon.exe.4fa0000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.nanocore.exe.58b0000.12.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.1.nanocore.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.nanocore.exe.6fc70000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
8.2.nanocore.exe.6eec0000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
9.2.dhcpmon.exe.6eda0000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
11.1.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.dhcpmon.exe.6f650000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
11.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.1.nanocore.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.1.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
chinomso.duckdns.org	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
chinomso.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chinomso.duckdns.org	213.208.152.210	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
chinomso.duckdns.org	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.208.152.210	chinomso.duckdns.org	Austria		1764	NEXTLAYER-ASAT	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384377
Start date:	09.04.2021
Start time:	01:07:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nanocore.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/20@24/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.1% (good quality ratio 10.2%) • Quality average: 76.5% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 23.54.113.45, 23.54.113.53, 104.43.139.144, 168.61.161.212, 13.64.90.137, 52.255.188.83, 20.82.210.154, 23.10.249.26, 23.10.249.43, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
01:08:01	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\nanocore.exe" s>$(Arg0)
01:08:01	API Interceptor	1034x Sleep call for process: nanocore.exe modified
01:08:02	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
01:08:04	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
213.208.152.210	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	Uv8hwOAKgm.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
chinomso.duckdns.org	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 213.208.152.210
	Uv8hwOAKgm.exe	Get hash	malicious	Browse	• 213.208.152.210
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 98.143.144.221
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.150.24.55
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.150.24.55
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 185.150.24.55
	Ku2bTlXUN4.exe	Get hash	malicious	Browse	• 197.211.59.64
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 185.150.24.55
	CHEQUE COPY RECEIPT.exe	Get hash	malicious	Browse	• 185.150.24.55
	CHEQUE COPY.exe	Get hash	malicious	Browse	• 185.150.24.55
	PAYMENT COPY RECEIPT.exe	Get hash	malicious	Browse	• 185.150.24.55
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	DHL AWB TRACKING DETAIL.exe	Get hash	malicious	Browse	• 194.5.98.56
	odou7cg844.exe	Get hash	malicious	Browse	• 129.205.124.145
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.244.30.86

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NEXTLAYER-ASAT	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 213.208.152.210
	Uv8hwOAKgm.exe	Get hash	malicious	Browse	• 213.208.152.210
	index_2021-03-02-12_11.dll	Get hash	malicious	Browse	• 213.208.134.178
	AI5aGob7HV.dll	Get hash	malicious	Browse	• 213.208.134.178
	SkQguXQerV.dll	Get hash	malicious	Browse	• 213.208.134.178
	LVFIZ8uZzp.dll	Get hash	malicious	Browse	• 213.208.134.178
	Statement as of_03_01_2021.xlsm	Get hash	malicious	Browse	• 213.208.134.178
	printouts_of_outstanding_as_of_mar_01_2021.xlsm	Get hash	malicious	Browse	• 213.208.134.178
	A43zoxMv6x.dll	Get hash	malicious	Browse	• 213.208.134.178
	2rS70o1G3T.dll	Get hash	malicious	Browse	• 213.208.134.178
	eXeMEWy2CI.dll	Get hash	malicious	Browse	• 213.208.134.178
	3TWrYtkzly.dll	Get hash	malicious	Browse	• 213.208.134.178
	Statement_of_Account_as_of_mar_01_2021.xlsm	Get hash	malicious	Browse	• 213.208.134.178
	index_2021-03-01-17_13.dll	Get hash	malicious	Browse	• 213.208.134.178
	printouts_of_outstanding_as_of_03_01_2021.xlsm	Get hash	malicious	Browse	• 213.208.134.178
	DZoj4wicd0.dll	Get hash	malicious	Browse	• 213.208.134.178
	uwq8T3mqDx.dll	Get hash	malicious	Browse	• 213.208.134.178
	E2uiGA3X2v.dll	Get hash	malicious	Browse	• 213.208.134.178
	RjIx2AoDBJ.dll	Get hash	malicious	Browse	• 213.208.134.178
	v2dw80uF0x.dll	Get hash	malicious	Browse	• 213.208.134.178

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\nanocore.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	321222
Entropy (8bit):	7.952258735347819
Encrypted:	false
SSDEEP:	6144:HdlwCtaK8BqoNWDCANNpFONOXopiTgRXWTZU3qC4XpO5BDiQ2KHeG:/xtaR0oQDCANPYNNpUDJX45BkEeG
MD5:	08803CC817D8B1046A964AF11685B15C
SHA1:	8D76CC9E4E21F90AAA0D2A8E9DD88CCB03349F29
SHA-256:	00343EF156007C41A76ABEBE2B0304AACC7E2B12E0D30EA476ECF8C847A54DFC
SHA-512:	BF548910BE04B74D3A8BF8F058D642DAC070D0CC94CA4EAC04EBC4341967ACFD65E5B64232BE0345994B05A847C7501C122D6F70AEB1FE7121BC8F093028C2 3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 34%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H.....,.....:..!.....&.....e.....Rich.....PE..L.....8E .....Z....9.....J1.....p....@.....:.....Ds.....:.....p.....text....Y.... ...Z..... ..`.rdata.....p.....^.....@..@.data...4.9.....p.....@....ndata.....@:.....rsrc.....:.....t.....@..@..... ....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\nanocore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F 8
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nanocore.exe.log	
Process:	C:\Users\user\Desktop\nanocore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	279040
Entropy (8bit):	**7.999366542899994**
Encrypted:	**true**
SSDEEP:	6144:BtaK8BqoNWDCANNpFONOXopiTgRXWTZU3qC4XpO5BDiQ2KH5:BtaR0oQDCANPYNNpUDJX45BkE5
MD5:	87317BA0D399E3C709FEE0DD272B7ED2
SHA1:	7A5685DA841B945A6B73BD383D05A83357317296
SHA-256:	96C109DF379172E6953F1E7F38B8C2A638989012662ACDE523BDB7E955F80B68
SHA-512:	8A93D135BD61C1CF00EA7A5E6CCC87BC84C050BE501B3E89829C759463002CFE7B62E52A7C48D1A391BDCF6311014107F8888A81CAFAD4E90B687052389C616
Malicious:	false
Reputation:	low
Preview:	..x.].].#..o,s:.'...\.X.,.....O...V....'*...%..W\.L..j...j..0+.....s2u..;.....q>..Q>.R.-...'...h.'/)Z.0....Bc.[.P.).$!p...S...@D.`I?."N7.59@.6&=A#&.....9.....,..mmj_.).3.s._4.7..N...L. .$.U..k.g..3..#X.....1...i...s.....sD...P...,.g.T..v{A.+.}_:..(2.%.Y.].N...Y.b.,l...^...-jAP@ik.p0l.J{6.K.6.A..>..5...A.$'....lhR 0...pn.+....0.....v..LD....>..a...G.Z.....,..Bh..F.}.pY. b0<... ...R=.n..{xV.2}..Y.....*h6Y@.._.+K.S%.../...DP..G....4x.....t..=..p..Z....oH.mG..g...d..z.v.E.g.%.....w.d.....<.....j..j.AH....F.1...lY.oWb.F.....w[...A.J[du.....QK.j.:..,..h;F..H ..],.92v..1....PB.V.H..t...4..b.....s.6..3Go...b...U...EF .....H.Q7...s...M).00.f\3 ..i..u..=...p...zp.....H.H..t..].....b.f.\n..H.Q-w..S...6....L....4.'1.u....1..b.....<..2}....@..6..-.....'\..l% .Q.x...^7.x..`.. ....ux.!3[..o<.....D...L.>l.....}sy....$.|.W....p..$0.sH94..rE.....b..U[.!.....A.....j.z.eD...d.O'.....".os.}D..oG....1.D...P2~KJ..a..d...u.

C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.968813365057691
Encrypted:	false
SSDEEP:	96:vQgv6/j3/PiDWkEusDpXtPYTTHfQk01XYNqHhf3/pQI1opkSuWIxMuOpmAd7g:Y9TNDNtPTGNqHhfRQDNIxSpmsk
MD5:	524E815672556CC3AA17CD643C9A351B
SHA1:	49CF76A2F0F2154A7D81D0800DA2B91F0B470DAA
SHA-256:	0F511CF2EAF33C2F20F912E88EBC0A4421780CDDC561C0AE8512E97EEFDF2A70
SHA-512:	BDCCA0642C4EA27FD4ED06411657EBD2665CF9BBA06FB84DEB68AF6DF387FDD4F932E423006B409B424A45B1B94E6CEEF0CF384F46BF86E181F9FF2298A39D23
Malicious:	false

C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	
Preview:	.MlN...P..cN.*....o%.vP..*...9/.....m6.!.....T"b.....(d..@J.zNL..rVz.....Q.._AAA..?Ry9.....e..rXWj..T^t8..&...u..qO.c..eZs3.....Y.LV.X..f>>.....Y.Ke.=..kRE..>.".U.F\.N..hFx. ../...m..=kd_".yJ?.... .I.@but5.zFR...L{8.....-..8...7.B.I.JE..p.r;.|.3.6.....0.E.7.EZ..E.]$.{.....p.{.@G4..4.....\|FAH..V.N:..D.....{U.M..[.u5..$.....vlN^..X.H4....%...m[TO.. i.o/.....pReD%.j.B....+...GYVY..g.A....]R.....9.Q3.....vO...H...@b.....R.....k_..R.~&E....Q.(Oa..N..I.R..M.,Sa..j.0.^*8.i.....&j..+-...e.Gs0....l^..D..!..P.)#>z.`.`..lb.....Z^.h;|..p B`<.X...r.7nK.5u..l.%_%v..J[.1q...s3....q...;h..0*....m.%.....HO..G.0.E....".#.....z[..A.9~C..&...+...0~.yc?.....Y:Fo=.....H.6JR..T@.~(....D}.xNh....._..cOL..MK...=.....s+ F...V.....@..&..%~..yF..no.6.a!....$7...z..`]....}:...aI_.:...yy..?...L..u...S5..1r...{%..tq..].1.s3.....m..,\....*...o.II.-EK.....e..T.K.\...Xq..UP....."........z..@.\.`iK...E J\

C:\Users\user\AppData\Local\Temp\nse444B.tmp\4rmzuajr4dtt.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.188029460900488
Encrypted:	false
SSDEEP:	48:StRJBN/SHIPAK6v5PXha+HGLFHIPAROGa4zzBvoAXAdUMQ9BgqRuqS:GN/KIZ6xYLlhGXHBgVueKx
MD5:	422D5CA3EDC5BA6E946720C8E1FD69F9
SHA1:	8009E5F7EF9CF4B43DE28D8A11048C195A887EE7
SHA-256:	4D78BB146725F4E19EC267E7DDDC6074F99561482693C6F0CF2C0C64A9EA76A1
SHA-512:	6B3B67C076EE5E61C1EC196D117FF564E7302256C20342750F8CAE761CDE76231B309AEF3A002FD9F0474BDA658DF80577A273EEF30387DE1C56013BD89100E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L.....n`.....!..... ..... .....`.....@.....0!..T...p".....@.....P..p....!..... ....text..... ..`.rdata..@.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsj42E4.tmp\4rmzuajr4dtt.dll	
Process:	C:\Users\user\Desktop\nanocore.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.188029460900488
Encrypted:	false
SSDEEP:	48:StRJBN/SHIPAK6v5PXha+HGLFHIPAROGa4zzBvoAXAdUMQ9BgqRuqS:GN/KIZ6xYLlhGXHBgVueKx
MD5:	422D5CA3EDC5BA6E946720C8E1FD69F9
SHA1:	8009E5F7EF9CF4B43DE28D8A11048C195A887EE7
SHA-256:	4D78BB146725F4E19EC267E7DDDC6074F99561482693C6F0CF2C0C64A9EA76A1
SHA-512:	6B3B67C076EE5E61C1EC196D117FF564E7302256C20342750F8CAE761CDE76231B309AEF3A002FD9F0474BDA658DF80577A273EEF30387DE1C56013BD89100E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L.....n`.....!..... ..... .....`.....@.....0!..T...p".....@.....P..p....!..... ....text..... ..`.rdata..@.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsn2692.tmp\4rmzuajr4dtt.dll	
Process:	C:\Users\user\Desktop\nanocore.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.188029460900488
Encrypted:	false
SSDEEP:	48:StRJBN/SHIPAK6v5PXha+HGLFHIPAROGa4zzBvoAXAdUMQ9BgqRuqS:GN/KIZ6xYLlhGXHBgVueKx
MD5:	422D5CA3EDC5BA6E946720C8E1FD69F9
SHA1:	8009E5F7EF9CF4B43DE28D8A11048C195A887EE7
SHA-256:	4D78BB146725F4E19EC267E7DDDC6074F99561482693C6F0CF2C0C64A9EA76A1
SHA-512:	6B3B67C076EE5E61C1EC196D117FF564E7302256C20342750F8CAE761CDE76231B309AEF3A002FD9F0474BDA658DF80577A273EEF30387DE1C56013BD89100E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L.....n`.....!..... ..... .....`.....@.....0!..T...p".....@.....P..p....!..... ....text..... ..`.rdata..@.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsq6D11.tmp\4rmzuajr4dtt.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.188029460900488
Encrypted:	false
SSDEEP:	48:StRJBN/SHIPAK6v5PXha+HGLFHIPAROGa4zzBvoAXAdUMQ9BgqRuqS:GN/KIZ6xYLlhGXHBgVueKx
MD5:	422D5CA3EDC5BA6E946720C8E1FD69F9
SHA1:	8009E5F7EF9CF4B43DE28D8A11048C195A887EE7
SHA-256:	4D78BB146725F4E19EC267E7DDDC6074F99561482693C6F0CF2C0C64A9EA76A1
SHA-512:	6B3B67C076EE5E61C1EC196D117FF564E7302256C20342750F8CAE761CDE76231B309AEF3A002FD9F0474BDA658DF80577A273EEF30387DE1C56013BD89100E7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L.....n`.....!..... ..... .....`.....@.....0!..T...p".....@.....P..p....!..... ....text..... ..`.rdata..@.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tmp38C1.tmp	
Process:	C:\Users\user\Desktop\nanocore.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1298
Entropy (8bit):	5.088310480171837
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Y+xtn:cbk4oL600QydbQxIYODOLedq3yj
MD5:	E9CED5EE66F06173F8F3B092B79010DE
SHA1:	BC76BE5331F85F7578FD935962AC9B33CC2B4C84
SHA-256:	4660276EA7A477C5FFCA499897DED1F46699637D3BC1BEA135A81CDE2D65E597
SHA-512:	4358E09932D6C4C95A75DC5C9DE1EE7DA6ABE286C9D28C85034261EB1CA37432FAAAC2565CF8132314926B6EDD41DD508F1CC3212EA2D72C098C3219878963B
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\tmp3B81.tmp	
Process:	C:\Users\user\Desktop\nanocore.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:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
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\nanocore.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:rHn:rH
MD5:	6E43C715DA3279FF2D19AACEF5CFA286
SHA1:	0FEE17EEE58CC51B81398326AB1780256AFB4CC4
SHA-256:	17C98C9953D73CDD75CC7FBC761A9FFB005F6D9C941EE28E3453DBA820ED9257
SHA-512:	8E4C1688E2204B5EDD87F277D2211352AFD8CC9CE9F001ACFAEA6791528E5B165B8CA643074B872E2127370F84125860C4413381DBCFFAB0F77C13FF7DF31EC
Malicious:	**true**
Preview:	.%+'...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\nanocore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	35
Entropy (8bit):	3.807435516759526
Encrypted:	false
SSDEEP:	3:oNt+WfWLi4dAn:oNwvpAn
MD5:	D43FC6D6883371ADF56312C5835AA391
SHA1:	F520273107B3112B206695814B60A3B99C3AA771
SHA-256:	E311EE9579E921EEBC32D2777133129FF0D961E445A47AD10E01724A4BC40040
SHA-512:	B058B33D57B6340DA0FFEC04B5129C6B20F93C426C51D660B97A2067D9AAF27D7431A5E04FB1A1B078B3B006DF8BE6407E03DA2199090ECF7519267F3BE6649(
Malicious:	false
Preview:	C:\Users\user\Desktop\nanocore.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.952258735347819
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	nanocore.exe
File size:	321222
MD5:	08803cc817d8b1046a964af11685b15c
SHA1:	8d76cc9e4e21f90aaa0d2a8e9dd88ccb03349f29
SHA256:	00343ef156007c41a76abebe2b0304aacc7e2b12e0d30ea476ecf8c847a54dfc
SHA512:	bf548910be04b74d3a8bf8f058d642dac070d0cc94ca4eac04ebc4341967acfd65e5b64232be0345994b05a847c7501c122d6f70aeb1fe7121bc8f093028c2f3
SSDEEP:	6144:HdlwCtaK8BqoNWDCANNpFONOXopiTgRXWTZU3qC4XpO5BDiQ2KHeG:/xtaR0oQDCANPYNNpUDJX45BkEeG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H.....,.....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 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:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007F08B8C3BAE8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F08B8C39229h
test eax, eax
jne 00007F08B8C392E6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F08B8C3BAD3h
call 00007F08B8C39209h
test eax, eax
je 00007F08B8C39402h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]

Instruction
push eax
push edi
call 00007F08B8C3BA91h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F08B8C392CCh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 111

- 53 (DNS)
- 7688 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 01:08:02.280957937 CEST	49740	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:02.303638935 CEST	7688	49740	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:02.811045885 CEST	49740	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:02.834539890 CEST	7688	49740	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:03.342253923 CEST	49740	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:03.365015030 CEST	7688	49740	213.208.152.210	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 01:08:07.644037962 CEST	49746	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:07.667594910 CEST	7688	49746	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:08.186372995 CEST	49746	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:08.209548950 CEST	7688	49746	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:08.717704058 CEST	49746	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:08.740946054 CEST	7688	49746	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:12.804413080 CEST	49747	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:12.829931021 CEST	7688	49747	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:13.343116999 CEST	49747	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:13.366044044 CEST	7688	49747	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:13.874443054 CEST	49747	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:13.897789955 CEST	7688	49747	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:17.966085911 CEST	49750	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:17.989341021 CEST	7688	49750	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:18.499778986 CEST	49750	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:18.522970915 CEST	7688	49750	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:19.077910900 CEST	49750	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:19.100735903 CEST	7688	49750	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:23.326785088 CEST	49752	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:23.350080967 CEST	7688	49752	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:23.984529018 CEST	49752	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:24.007906914 CEST	7688	49752	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:24.672143936 CEST	49752	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:24.695725918 CEST	7688	49752	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:28.920422077 CEST	49753	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:28.944849014 CEST	7688	49753	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:29.453850985 CEST	49753	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:29.476957083 CEST	7688	49753	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:29.985090971 CEST	49753	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:30.008549929 CEST	7688	49753	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:34.066354990 CEST	49754	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:34.090085983 CEST	7688	49754	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:34.594835997 CEST	49754	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:34.618825912 CEST	7688	49754	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:35.126112938 CEST	49754	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:35.149136066 CEST	7688	49754	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:39.199570894 CEST	49759	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:39.222735882 CEST	7688	49759	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:39.735841036 CEST	49759	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:39.761449099 CEST	7688	49759	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:40.267229080 CEST	49759	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:40.291462898 CEST	7688	49759	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:44.334249973 CEST	49767	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:44.357805967 CEST	7688	49767	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:44.861443043 CEST	49767	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:44.884512901 CEST	7688	49767	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:45.392525911 CEST	49767	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:45.415189028 CEST	7688	49767	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:49.506330013 CEST	49768	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:49.529818058 CEST	7688	49768	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:50.033529043 CEST	49768	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:50.057566881 CEST	7688	49768	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:50.564888954 CEST	49768	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:50.588016033 CEST	7688	49768	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:54.667339087 CEST	49769	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:54.690824032 CEST	7688	49769	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:55.206002951 CEST	49769	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:55.229613066 CEST	7688	49769	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:55.737279892 CEST	49769	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:55.759967089 CEST	7688	49769	213.208.152.210	192.168.2.4
Apr 9, 2021 01:08:59.863363981 CEST	49770	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:08:59.887548923 CEST	7688	49770	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:00.393878937 CEST	49770	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:00.417368889 CEST	7688	49770	213.208.152.210	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 01:09:00.925184965 CEST	49770	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:00.952183962 CEST	7688	49770	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:05.483297110 CEST	49771	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:05.506546021 CEST	7688	49771	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:06.019205093 CEST	49771	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:06.042946100 CEST	7688	49771	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:06.550513029 CEST	49771	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:06.573656082 CEST	7688	49771	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:10.629232883 CEST	49772	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:10.652252913 CEST	7688	49772	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:11.160331964 CEST	49772	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:11.186142921 CEST	7688	49772	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:11.691643953 CEST	49772	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:11.714682102 CEST	7688	49772	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:15.971256018 CEST	49773	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:15.994257927 CEST	7688	49773	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:16.504492998 CEST	49773	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:16.528068066 CEST	7688	49773	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:17.035680056 CEST	49773	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:17.061697006 CEST	7688	49773	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:21.116499901 CEST	49774	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:21.140182972 CEST	7688	49774	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:21.645622969 CEST	49774	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:21.668996096 CEST	7688	49774	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:22.176837921 CEST	49774	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:22.199614048 CEST	7688	49774	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:26.495048046 CEST	49777	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:26.520327091 CEST	7688	49777	213.208.152.210	192.168.2.4
Apr 9, 2021 01:09:27.020973921 CEST	49777	7688	192.168.2.4	213.208.152.210
Apr 9, 2021 01:09:27.043709040 CEST	7688	49777	213.208.152.210	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 01:07:48.308937073 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:48.322262049 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:48.703804016 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:48.735263109 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:49.046216011 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:49.058747053 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:49.125768900 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:49.147308111 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:49.767405987 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:49.780075073 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:50.543967009 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:50.564155102 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:51.460773945 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:51.473685026 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:52.154879093 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:52.167908907 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:52.906627893 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:52.919509888 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:53.756854057 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:53.770009041 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:55.434540987 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:55.446664095 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:56.471210957 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:56.483896971 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:57.667022943 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:57.681679010 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 9, 2021 01:07:59.537436962 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:07:59.550411940 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:00.450153112 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:00.463025093 CEST	53	53700	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 01:08:01.468883991 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:01.481945992 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:02.088749886 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:02.262785912 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:02.270627022 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:02.277312040 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:03.587178946 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:03.600624084 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:04.384593964 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:04.397150040 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:05.193519115 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:05.205976963 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:06.646678925 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:06.660923958 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:07.447942972 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:07.633944988 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:12.788408995 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:12.802980900 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:16.958344936 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:16.971411943 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:17.934674978 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:17.947594881 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:22.457528114 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:22.475927114 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:23.145405054 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:23.325608969 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:28.906090975 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:28.918818951 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:34.050785065 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:34.064754963 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:37.794886112 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:37.885232925 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:38.373080015 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:38.449672937 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:38.889656067 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:38.904063940 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:39.167108059 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:39.185307980 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:39.193701029 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:39.198570967 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:39.252386093 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:39.358108997 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:39.769283056 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:39.782944918 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:40.212387085 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:40.226979017 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:40.567267895 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:40.584165096 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:41.188708067 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:41.201442957 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:41.898530960 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:41.913628101 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:42.309269905 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:42.322654009 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:44.320179939 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:44.333240032 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:49.492639065 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:49.505250931 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:54.652204037 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:54.665515900 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 9, 2021 01:08:59.848192930 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:08:59.861691952 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:05.433816910 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:05.449538946 CEST	53	57525	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 01:09:10.603766918 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:10.616873980 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:15.773886919 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:15.968554020 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:21.101937056 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:21.115186930 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:23.917705059 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:23.930465937 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:26.312844038 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:26.494016886 CEST	53	49944	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:26.608517885 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:26.622071981 CEST	53	63300	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:31.624968052 CEST	61449	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:31.638266087 CEST	53	61449	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:36.777276993 CEST	51275	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:36.790810108 CEST	53	51275	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:42.026740074 CEST	63492	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:42.040246010 CEST	53	63492	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:47.194799900 CEST	58945	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:47.376025915 CEST	53	58945	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:52.566468000 CEST	60779	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:52.581572056 CEST	53	60779	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:57.700588942 CEST	64014	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:57.713606119 CEST	53	64014	8.8.8.8	192.168.2.4
Apr 9, 2021 01:09:57.835365057 CEST	57091	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:09:57.847999096 CEST	53	57091	8.8.8.8	192.168.2.4
Apr 9, 2021 01:10:02.821433067 CEST	55904	53	192.168.2.4	8.8.8.8
Apr 9, 2021 01:10:02.834716082 CEST	53	55904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 01:08:02.088749886 CEST	192.168.2.4	8.8.8.8	0x5006	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:07.447942972 CEST	192.168.2.4	8.8.8.8	0x5666	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:12.788408995 CEST	192.168.2.4	8.8.8.8	0x54e2	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:17.934674978 CEST	192.168.2.4	8.8.8.8	0xca88	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:23.145405054 CEST	192.168.2.4	8.8.8.8	0xa922	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:28.906090975 CEST	192.168.2.4	8.8.8.8	0x556c	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:34.050785065 CEST	192.168.2.4	8.8.8.8	0x5972	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:39.185307980 CEST	192.168.2.4	8.8.8.8	0x9ea3	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:44.320179939 CEST	192.168.2.4	8.8.8.8	0x5c7a	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:49.492639065 CEST	192.168.2.4	8.8.8.8	0x5d10	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:54.652204037 CEST	192.168.2.4	8.8.8.8	0x719d	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:59.848192930 CEST	192.168.2.4	8.8.8.8	0x5d95	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:05.433816910 CEST	192.168.2.4	8.8.8.8	0xd355	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:10.603766918 CEST	192.168.2.4	8.8.8.8	0x6528	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:15.773886919 CEST	192.168.2.4	8.8.8.8	0xb0e7	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:21.101937056 CEST	192.168.2.4	8.8.8.8	0x711b	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:26.312844038 CEST	192.168.2.4	8.8.8.8	0x6f6e	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:31.624968052 CEST	192.168.2.4	8.8.8.8	0x84a2	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 01:09:36.777276993 CEST	192.168.2.4	8.8.8.8	0x2cac	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:42.026740074 CEST	192.168.2.4	8.8.8.8	0xae6a	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:47.194799900 CEST	192.168.2.4	8.8.8.8	0x5a3c	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:52.566468000 CEST	192.168.2.4	8.8.8.8	0x90a0	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:57.700588942 CEST	192.168.2.4	8.8.8.8	0x219b	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Apr 9, 2021 01:10:02.821433067 CEST	192.168.2.4	8.8.8.8	0x2c4b	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

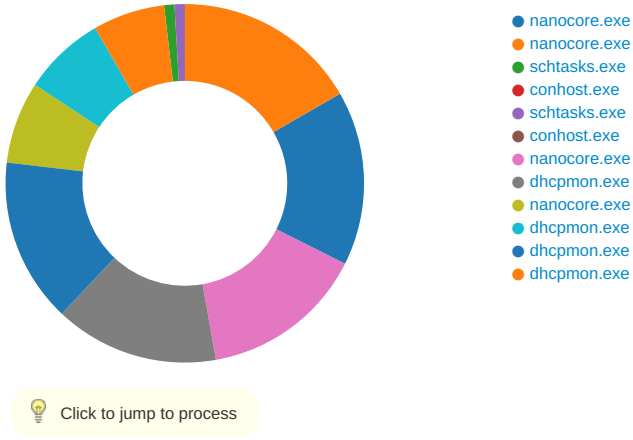
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 01:08:02.270627022 CEST	8.8.8.8	192.168.2.4	0x5006	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:07.633944988 CEST	8.8.8.8	192.168.2.4	0x5666	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:12.802980900 CEST	8.8.8.8	192.168.2.4	0x54e2	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:17.947594881 CEST	8.8.8.8	192.168.2.4	0xca88	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:23.325608969 CEST	8.8.8.8	192.168.2.4	0xa922	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:28.918818951 CEST	8.8.8.8	192.168.2.4	0x556c	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:34.064754963 CEST	8.8.8.8	192.168.2.4	0x5972	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:39.198570967 CEST	8.8.8.8	192.168.2.4	0x9ea3	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:44.333240032 CEST	8.8.8.8	192.168.2.4	0x5c7a	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:49.505250931 CEST	8.8.8.8	192.168.2.4	0x5d10	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:54.665515900 CEST	8.8.8.8	192.168.2.4	0x719d	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:08:59.861691952 CEST	8.8.8.8	192.168.2.4	0x5d95	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:05.449538946 CEST	8.8.8.8	192.168.2.4	0xd355	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:10.616873980 CEST	8.8.8.8	192.168.2.4	0x6528	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:15.968554020 CEST	8.8.8.8	192.168.2.4	0xb0e7	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:21.115186930 CEST	8.8.8.8	192.168.2.4	0x711b	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:26.494016886 CEST	8.8.8.8	192.168.2.4	0x6f6e	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:31.638266087 CEST	8.8.8.8	192.168.2.4	0x84a2	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:36.790810108 CEST	8.8.8.8	192.168.2.4	0x2cac	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:42.040246010 CEST	8.8.8.8	192.168.2.4	0xae6a	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 01:09:47.376025915 CEST	8.8.8.8	192.168.2.4	0x5a3c	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:52.581572056 CEST	8.8.8.8	192.168.2.4	0x90a0	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:09:57.713606119 CEST	8.8.8.8	192.168.2.4	0x219b	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)
Apr 9, 2021 01:10:02.834716082 CEST	8.8.8.8	192.168.2.4	0x2c4b	No error (0)	chinomso.duckdns.org		213.208.152.210	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: nanocore.exe PID: 7064 Parent PID: 5956

General

Start time:	01:07:54
Start date:	09/04/2021
Path:	C:\Users\user\Desktop\nanocore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nanocore.exe'
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.651116412.000000001EEC0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nss2662.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsn2692.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsn2692.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsn2692.tmp\4rmzuajr4dtt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nss2662.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsn2692.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	ea 4d 6c 4e 93 b6 c8 50 ee 01 63 4e f3 bc 2a b0 ef e6 10 6f 25 0c 76 50 00 dd 2a 8b f0 e9 39 2f dd e6 d9 1d bc e0 6d 36 a9 21 03 af f4 e6 c6 00 df 54 22 62 fa 04 1c 07 95 e0 28 64 a1 04 40 4a 98 7a 4e 4c fd b5 72 56 7a 1e e0 bf 84 c2 83 03 d9 51 fa ba 5f 41 41 41 08 9c 3f 52 79 39 f9 c2 1b cd 98 fe da 65 f7 b7 72 58 57 6a 13 9b 54 5e 74 38 f2 cd 26 d0 a5 11 d7 75 f4 b4 71 4f fb 63 0e a2 65 5a 73 33 ef d0 a6 db 96 14 ec 59 ed ad 4c 56 12 58 11 a9 66 3e 3e 0a cc d3 12 d6 a7 0f cd 59 c6 86 4b 65 fe 3d 04 90 6b 52 45 05 c5 be 3e e1 9c 22 de 55 cb 8b 46 5c dd 4e ff a7 68 46 78 04 be d9 2f ec b9 15 e3 6d c0 80 3d 6b 64 5f 22 9e 79 4a 3f ff f3 e4 a0 e7 a2 20 d0 49 d9 99 40 62 75 74 35 9d 7a 46 52 16 d8 ad a5 4c 7b 38 02 18 d2 92 0c fe 2d c5 f4 87 38 cb af be af	.MlN...P..cN..*....o%.vP..*.. .9/.....m6.!.....T"b.....(d ..@J.zNL..rVz.....Q.._AA A..? Ry9.....e..rXWj..T^t8..&... .u..qO.c..eZs3.....Y..LV.X. . f>>.....Y..Ke.=..kRE...>.." .U..F\.N..hFx.../....m..=kd_" .yJ?..... .I..@but5.zFR....L{8.....- ...8....	success or wait	1	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	32768	87 c8 78 93 5d e6 5d 0f 23 8d 8f 6f 2c 73 3a 0d 27 ab da e0 5c c5 58 85 2c 90 ab a1 8d b1 b6 4f a5 14 e7 a6 56 f6 e0 98 18 27 2a f9 a8 db 25 ab 05 57 5c ed 4c 17 d3 6a b3 88 9d 6a ad 9f 30 2b 06 a9 1d 11 85 09 73 32 75 b8 e4 3b b4 1c aa b2 c6 d2 71 3e b2 df 51 3e 1e 52 f5 2d 1f 86 be 27 a7 02 ac 68 a9 27 2f 29 5a 18 30 bf 83 9c e3 42 63 89 5b f4 50 dd 9b 29 84 24 21 70 05 af bc 53 f9 7f 1c 40 44 c3 60 49 3f ad 22 4e 37 f0 35 39 40 f5 36 26 3d 41 23 26 8b 1c f3 ae a2 cf 92 fd b9 e8 39 f8 0b ef c1 0e e3 2c 90 e5 6d 6d 6a 5f e4 29 0f 33 e3 73 ab 5f 34 d4 37 9c 10 4e 1a 7f cf 4c 16 d9 24 00 55 a4 c8 6b d5 67 89 9e 33 19 c7 23 58 92 93 97 ed c3 a5 bf ca c0 8e 82 31 7f cc 8d ad 69 0c 8f 10 73 04 11 89 9a 94 00 eb 73 44 8c f3 fa 50 a4 c9 c0 2c dc 67 db 54 1d e6	..x.].].#..o,s:.'...\.X.,..... .O....V....'*...%..W\.L..j...j ..0+......s2u..;......q>..Q>.R .-...'...h.'/)Z.0....Bc.[.P..) .$!p...S...@D.`I?."N7.59@. 6&=A #&..........9......,..mmj_.).3 .s._4.7..N...L..$.U..k.g..3..# X...........1....i...s.......s D...P...,.g.T..	success or wait	9	403091	WriteFile
C:\Users\user\AppData\Local\Temp\nsn2692.tmp\4rmzuajr4dtt.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 91 8b 6e 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L.....n`...........!	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\nanocore.exe	unknown	512	success or wait	73	4030EA	ReadFile
C:\Users\user\Desktop\nanocore.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\nanocore.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	success or wait	1	6FC710B0	ReadFile
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	279040	success or wait	1	2CB15E1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile

Analysis Process: nanocore.exe PID: 7104 Parent PID: 7064

General

Start time:	01:07:55
Start date:	09/04/2021
Path:	C:\Users\user\Desktop\nanocore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nanocore.exe'
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
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: 00000002.00000002.904801478.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.904801478.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.904801478.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.904801478.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.909694649.00000000058B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.909694649.00000000058B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.909694649.00000000058B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.907930500.0000000004A92000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.907930500.0000000004A92000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.907930500.0000000004A92000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.905801654.0000000002531000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.904977643.0000000000598000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.904977643.0000000000598000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.904977643.0000000000598000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.909667904.0000000005820000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.909667904.0000000005820000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000001.645917465.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000001.645917465.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000001.645917465.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.907047589.0000000004970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.907047589.0000000004970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.907047589.0000000004970000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.907047589.0000000004970000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.906581049.00000000035AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.906581049.00000000035AC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D23CF06	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	6D23CF06	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	6BFABEFF	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	6BFA1E60	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	6BFABEFF	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	6BFADD66	CopyFileW
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	6BFADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp38C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFA7038	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	6BFA1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3B81.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFA7038	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	6BFABEFF	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	6BFABEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp38C1.tmp	success or wait	1	6BFA6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp3B81.tmp	success or wait	1	6BFA6A95	DeleteFileW
C:\Users\user\Desktop\nanocore.exe:Zone.Identifier	success or wait	1	5288BA6	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	unknown	8	e0 25 2b 27 e3 fa d8 48	.%+'...H	success or wait	1	6BFA1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e6 64 96 48 a2 05 f8 1b a2 05 f8 1b a2 05 f8 1b 2c 0d a7 1b a0 05 f8 1b a2 05 f9 1b 3a 05 f8 1b 21 0d a5 1b b3 05 f8 1b f6 26 c8 1b a9 05 f8 1b 65 03 fe 1b a3 05 f8 1b 52 69 63 68 a2 05 f8 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0b cd 38 45 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5a 00 00 00 c6 39 00 00 04 00 00 4a 31 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........d.H............,..... ......:...!........&......e... ....Rich....................PE ..L.....8E.................Z.. ..9.....J1.....	success or wait	3	6BFADD66	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	6BFADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp38C1.tmp	unknown	1298	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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6BFA1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	35	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 6e 61 6e 6f 63 6f 72 65 2e 65 78 65	C:\Users\user\Desktop\nanocore.exe	success or wait	1	6BFA1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3B81.tmp	unknown	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	6BFA1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D215705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D21CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFA1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D1FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D1FD72F	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	6BFA646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 5800 Parent PID: 7104

General

Start time:	01:07:59
Start date:	09/04/2021
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\tmp38C1.tmp'
Imagebase:	0x1110000
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\tmp38C1.tmp	unknown	2	success or wait	1	111AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp38C1.tmp	unknown	1299	success or wait	1	111ABD9	ReadFile

Analysis Process: conhost.exe PID: 5820 Parent PID: 5800

General

Start time:	01:08:00
Start date:	09/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5108 Parent PID: 7104

General

Start time:	01:08:00
Start date:	09/04/2021
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\tmp3B81.tmp'
Imagebase:	0x1110000
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\tmp3B81.tmp	unknown	2	success or wait	1	111AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3B81.tmp	unknown	1311	success or wait	1	111ABD9	ReadFile

Analysis Process: conhost.exe PID: 4476 Parent PID: 5108

General

Start time:	01:08:00
Start date:	09/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: nanocore.exe PID: 4108 Parent PID: 968

General

Start time:	01:08:01
Start date:	09/04/2021
Path:	C:\Users\user\Desktop\nanocore.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\nanocore.exe 0
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.669624228.000000001EEC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.669624228.000000001EEC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.669624228.000000001EEC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.669624228.000000001EEC0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj42E3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj42E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj42E4.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj42E4.tmp\4rmzuajr4dtt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj42E3.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsj42E4.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	ea 4d 6c 4e 93 b6 c8 50 ee 01 63 4e f3 bc 2a b0 ef e6 10 6f 25 0c 76 50 00 dd 2a 8b f0 e9 39 2f dd e6 d9 1d bc e0 6d 36 a9 21 03 af f4 e6 c6 00 df 54 22 62 fa 04 1c 07 95 e0 28 64 a1 04 40 4a 98 7a 4e 4c fd b5 72 56 7a 1e e0 bf 84 c2 83 03 d9 51 fa ba 5f 41 41 41 08 9c 3f 52 79 39 f9 c2 1b cd 98 fe da 65 f7 b7 72 58 57 6a 13 9b 54 5e 74 38 f2 cd 26 d0 a5 11 d7 75 f4 b4 71 4f fb 63 0e a2 65 5a 73 33 ef d0 a6 db 96 14 ec 59 ed ad 4c 56 12 58 11 a9 66 3e 3e 0a cc d3 12 d6 a7 0f cd 59 c6 86 4b 65 fe 3d 04 90 6b 52 45 05 c5 be 3e e1 9c 22 de 55 cb 8b 46 5c dd 4e ff a7 68 46 78 04 be d9 2f ec b9 15 e3 6d c0 80 3d 6b 64 5f 22 9e 79 4a 3f ff f3 e4 a0 e7 a2 20 d0 49 d9 99 40 62 75 74 35 9d 7a 46 52 16 d8 ad a5 4c 7b 38 02 18 d2 92 0c fe 2d c5 f4 87 38 cb af be af	.MlN...P..cN..*....o%.vP..*.. .9/.....m6.!.....T"b.....(d ..@J.zNL..rVz.....Q.._AA A..? Ry9.....e..rXWj..T^t8..&... .u..qO.c..eZs3.....Y..LV.X. . f>>.....Y..Ke.=..kRE...>.." .U..F\.N..hFx.../....m..=kd_" .yJ?..... .l..@but5.zFR....L{8.....- ...8....	success or wait	1	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	32768	87 c8 78 93 5d e6 5d 0f 23 8d 8f 6f 2c 73 3a 0d 27 ab da e0 5c c5 58 85 2c 90 ab a1 8d b1 b6 4f a5 14 e7 a6 56 f6 e0 98 18 27 2a f9 a8 db 25 ab 05 57 5c ed 4c 17 d3 6a b3 88 9d 6a ad 9f 30 2b 06 a9 1d 11 85 09 73 32 75 b8 e4 3b b4 1c aa b2 c6 d2 71 3e b2 df 51 3e 1e 52 f5 2d 1f 86 be 27 a7 02 ac 68 a9 27 2f 29 5a 18 30 bf 83 9c e3 42 63 89 5b f4 50 dd 9b 29 84 24 21 70 05 af bc 53 f9 7f 1c 40 44 c3 60 49 3f ad 22 4e 37 f0 35 39 40 f5 36 26 3d 41 23 26 8b 1c f3 ae a2 cf 92 fd b9 e8 39 f8 0b ef c1 0e e3 2c 90 e5 6d 6d 6a 5f e4 29 0f 33 e3 73 ab 5f 34 d4 37 9c 10 4e 1a 7f cf 4c 16 d9 24 00 55 a4 c8 6b d5 67 89 9e 33 19 c7 23 58 92 93 97 ed c3 a5 bf ca c0 8e 82 31 7f cc 8d ad 69 0c 8f 10 73 04 11 89 9a 94 00 eb 73 44 8c f3 fa 50 a4 c9 c0 2c dc 67 db 54 1d e6	..x.].].#..o,s:.'...\.X.,..... .O....V....'*...%..W\.L..j...j ..0+......s2u..;......q>..Q>.R .-...'...h.'/)Z.0....Bc.[.P..) .$!p...S...@D.`I?."N7.59@. 6&=A #&..........9......,..mmj_.).3 .s._4.7..N...L..$.U..k.g..3..# X...........1....i...s.......s D...P...,.g.T..	success or wait	9	403091	WriteFile
C:\Users\user\AppData\Local\Temp\nsj42E4.tmp\4rmzuajr4dtt.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 91 8b 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L.....n`...........!	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\nanocore.exe	unknown	512	success or wait	73	4030EA	ReadFile
C:\Users\user\Desktop\nanocore.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\nanocore.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	success or wait	1	6EEC10B0	ReadFile
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	279040	success or wait	1	2CB15E1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2CB0871	ReadFile

Analysis Process: dhcpmon.exe PID: 5752 Parent PID: 968

General

Start time:	01:08:02
Start date:	09/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.671860077.000000001ED70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.671860077.000000001ED70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.671860077.000000001ED70000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.671860077.000000001ED70000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 34%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj441B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse444B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse444B.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse444B.tmp\4rmzuajr4dtt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj441B.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nse444B.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	ea 4d 6c 4e 93 b6 c8 50 ee 01 63 4e f3 bc 2a b0 ef e6 10 6f 25 0c 76 50 00 dd 2a 8b f0 e9 39 2f dd e6 d9 1d bc e0 6d 36 a9 21 03 af f4 e6 c6 00 df 54 22 62 fa 04 1c 07 95 e0 28 64 a1 04 40 4a 98 7a 4e 4c fd b5 72 56 7a 1e e0 bf 84 c2 83 03 d9 51 fa ba 5f 41 41 41 08 9c 3f 52 79 39 f9 c2 1b cd 98 fe da 65 f7 b7 72 58 57 6a 13 9b 54 5e 74 38 f2 cd 26 d0 a5 11 d7 75 f4 b4 71 4f fb 63 0e a2 65 5a 73 33 ef d0 a6 db 96 14 ec 59 ed ad 4c 56 12 58 11 a9 66 3e 3e 0a cc d3 12 d6 a7 0f cd 59 c6 86 4b 65 fe 3d 04 90 6b 52 45 05 c5 be 3e e1 9c 22 de 55 cb 8b 46 5c dd 4e ff a7 68 46 78 04 be d9 2f ec b9 15 e3 6d c0 80 3d 6b 64 5f 22 9e 79 4a 3f ff f3 e4 a0 e7 a2 20 d0 49 d9 99 40 62 75 74 35 9d 7a 46 52 16 d8 ad a5 4c 7b 38 02 18 d2 92 0c fe 2d c5 f4 87 38 cb af be af	.MlN...P..cN..*....o%.vP..*.. .9/.....m6.!.....T"b.....(d ..@J.zNL..rVz.....Q.._AA A..? Ry9.....e..rXWj..T^t8..&... .u..qO.c..eZs3.....Y..LV.X. . f>>.....Y..Ke.=..kRE...>.." .U..F\.N..hFx.../....m..=kd_" .yJ?..... .I..@but5.zFR....L{8.....- ...8....	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	32768	87 c8 78 93 5d e6 5d 0f 23 8d 8f 6f 2c 73 3a 0d 27 ab da e0 5c c5 58 85 2c 90 ab a1 8d b1 b6 4f a5 14 e7 a6 56 f6 e0 98 18 27 2a f9 a8 db 25 ab 05 57 5c ed 4c 17 d3 6a b3 88 9d 6a ad 9f 30 2b 06 a9 1d 11 85 09 73 32 75 b8 e4 3b b4 1c aa b2 c6 d2 71 3e b2 df 51 3e 1e 52 f5 2d 1f 86 be 27 a7 02 ac 68 a9 27 2f 29 5a 18 30 bf 83 9c e3 42 63 89 5b f4 50 dd 9b 29 84 24 21 70 05 af bc 53 f9 7f 1c 40 44 c3 60 49 3f ad 22 4e 37 f0 35 39 40 f5 36 26 3d 41 23 26 8b 1c f3 ae a2 cf 92 fd b9 e8 39 f8 0b ef c1 0e e3 2c 90 e5 6d 6d 6a 5f e4 29 0f 33 e3 73 ab 5f 34 d4 37 9c 10 4e 1a 7f cf 4c 16 d9 24 00 55 a4 c8 6b d5 67 89 9e 33 19 c7 23 58 92 93 97 ed c3 a5 bf ca c0 8e 82 31 7f cc 8d ad 69 0c 8f 10 73 04 11 89 9a 94 00 eb 73 44 8c f3 fa 50 a4 c9 c0 2c dc 67 db 54 1d e6	..x.].].#..o,s:.'...\.X.,..... .O....V....'*...%..W\.L..j...j ..0+.....s2u..;.....q>..Q>.R .-...'...h.'/)Z.0....Bc.[.P..) .$!p...S...@D.`I?."N7.59@. 6&=A #&.....9.....,..mmj_.).3 .s._4.7..N...L..$.U..k.g..3..# X.....1....i...s.....s D...P...,.g.T..	success or wait	9	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse444B.tmp\4rmzuajr4dtt.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 91 8b 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L.....n`...........!	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	512	success or wait	73	4030EA	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	success or wait	1	6EDA10B0	ReadFile
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	279040	success or wait	1	25415E1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2540871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2540871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2540871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2540871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2540871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2540871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2540871	ReadFile

Analysis Process: nanocore.exe PID: 5904 Parent PID: 4108

General

Start time:	01:08:02
Start date:	09/04/2021
Path:	C:\Users\user\Desktop\nanocore.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\nanocore.exe 0
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
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: 0000000A.00000002.683529518.0000000000679000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.683529518.0000000000679000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.683529518.0000000000679000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000001.662848703.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000001.662848703.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000001.662848703.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.684361480.0000000002510000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.684499268.00000000034FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.684499268.00000000034FC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.682558622.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.682558622.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.682558622.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.682558622.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.685817351.0000000004940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.685817351.0000000004940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.685817351.0000000004940000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.685817351.0000000004940000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.684426343.00000000034C1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.684426343.00000000034C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.684426343.00000000034C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.686102213.00000000049C2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.686102213.00000000049C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.686102213.00000000049C2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D23CF06	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	6D23CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nanocore.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D54C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nanocore.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D54C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D215705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D21CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFA1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6152 Parent PID: 5752

General

Start time:	01:08:03
Start date:	09/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.684555433.0000000002320000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.683969306.00000000006FC000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.683969306.00000000006FC000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.683969306.00000000006FC000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.683128059.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.683128059.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.683128059.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.683128059.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.686692380.0000000004922000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.686692380.0000000004922000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.686692380.0000000004922000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.684652674.000000000330C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.684652674.000000000330C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.686247080.00000000047F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.686247080.00000000047F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.686247080.00000000047F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.686247080.00000000047F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000001.663544913.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000001.663544913.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000001.663544913.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.684614120.00000000032D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.684614120.00000000032D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.684614120.00000000032D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D23CF06	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	6D23CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D54C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D54C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D215705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D21CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFA1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6724 Parent PID: 3424

General

Start time:	01:08:12
Start date:	09/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.691295579.000000001ED80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.691295579.000000001ED80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.691295579.000000001ED80000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.691295579.000000001ED80000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsq6D10.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsq6D11.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsq6D11.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsq6D11.tmp\4rmzuajr4dtt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq6D10.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsq6D11.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	ea 4d 6c 4e 93 b6 c8 50 ee 01 63 4e f3 bc 2a b0 ef e6 10 6f 25 0c 76 50 00 dd 2a 8b f0 e9 39 2f dd e6 d9 1d bc e0 6d 36 a9 21 03 af f4 e6 c6 00 df 54 22 62 fa 04 1c 07 95 e0 28 64 a1 04 40 4a 98 7a 4e 4c fd b5 72 56 7a 1e e0 bf 84 c2 83 03 d9 51 fa ba 5f 41 41 41 08 9c 3f 52 79 39 f9 c2 1b cd 98 fe da 65 f7 b7 72 58 57 6a 13 9b 54 5e 74 38 f2 cd 26 d0 a5 11 d7 75 f4 b4 71 4f fb 63 0e a2 65 5a 73 33 ef d0 a6 db 96 14 ec 59 ed ad 4c 56 12 58 11 a9 66 3e 3e 0a cc d3 12 d6 a7 0f cd 59 c6 86 4b 65 fe 3d 04 90 6b 52 45 05 c5 be 3e e1 9c 22 de 55 cb 8b 46 5c dd 4e ff a7 68 46 78 04 be d9 2f ec b9 15 e3 6d c0 80 3d 6b 64 5f 22 9e 79 4a 3f ff f3 e4 a0 e7 a2 20 d0 49 d9 99 40 62 75 74 35 9d 7a 46 52 16 d8 ad a5 4c 7b 38 02 18 d2 92 0c fe 2d c5 f4 87 38 cb af be af	.MlN...P..cN..*....o%.vP..*.. .9/.....m6.!.....T"b.....(d ..@J.zNL..rVz.....Q.._AA A..? Ry9.....e..rXWj..T^t8..&... .u..qO.c..eZs3.....Y..LV.X. . f>>.....Y..Ke.=..kRE...>.." .U..F\.N..hFx.../....m..=kd_" .yJ?..... .I..@but5.zFR....L{8.....- ...8....	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	32768	87 c8 78 93 5d e6 5d 0f 23 8d 8f 6f 2c 73 3a 0d 27 ab da e0 5c c5 58 85 2c 90 ab a1 8d b1 b6 4f a5 14 e7 a6 56 f6 e0 98 18 27 2a f9 a8 db 25 ab 05 57 5c ed 4c 17 d3 6a b3 88 9d 6a ad 9f 30 2b 06 a9 1d 11 85 09 73 32 75 b8 e4 3b b4 1c aa b2 c6 d2 71 3e b2 df 51 3e 1e 52 f5 2d 1f 86 be 27 a7 02 ac 68 a9 27 2f 29 5a 18 30 bf 83 9c e3 42 63 89 5b f4 50 dd 9b 29 84 24 21 70 05 af bc 53 f9 7f 1c 40 44 c3 60 49 3f ad 22 4e 37 f0 35 39 40 f5 36 26 3d 41 23 26 8b 1c f3 ae a2 cf 92 fd b9 e8 39 f8 0b ef c1 0e e3 2c 90 e5 6d 6d 6a 5f e4 29 0f 33 e3 73 ab 5f 34 d4 37 9c 10 4e 1a 7f cf 4c 16 d9 24 00 55 a4 c8 6b d5 67 89 9e 33 19 c7 23 58 92 93 97 ed c3 a5 bf ca c0 8e 82 31 7f cc 8d ad 69 0c 8f 10 73 04 11 89 9a 94 00 eb 73 44 8c f3 fa 50 a4 c9 c0 2c dc 67 db 54 1d e6	..x.].].#..o,s:.'...\.X.,..... .O....V....'*...%..W\.L..j...j ..0+.....s2u..;.....q>..Q>.R .-...'...h.'/)Z.0....Bc.[.P..) .$!p...S...@D.`I?."N7.59@. 6&=A #&.....9.....,..mmj_.).3 .s._4.7..N...L..$.U..k.g..3..# X.....1....i...s.....s D...P...,.g.T..	success or wait	9	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq6D11.tmp\4rmzuajr4dtt.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 91 8b 6e 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L.....n`...........!	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	512	success or wait	73	4030EA	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\ks446tcfy17w7jqy3r	unknown	6661	success or wait	1	6F6510B0	ReadFile
C:\Users\user\AppData\Local\Temp\6tts4zykw681emdi	unknown	279040	success or wait	1	2B715E1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70871	ReadFile

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

General

Start time:	01:08:13
Start date:	09/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x400000
File size:	321222 bytes
MD5 hash:	08803CC817D8B1046A964AF11685B15C
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: 0000000D.00000001.685346299.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000001.685346299.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000001.685346299.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.703714772.00000000033F1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.703714772.00000000033F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.703714772.00000000033F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.704559063.0000000004FA2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.704559063.0000000004FA2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.704559063.0000000004FA2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.703774283.000000000342C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.703774283.000000000342C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.702826612.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.702826612.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.702826612.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.702826612.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.703677926.0000000002440000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.703409413.00000000006E7000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.703409413.00000000006E7000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.703409413.00000000006E7000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.704356267.0000000004910000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.704356267.0000000004910000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.704356267.0000000004910000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.704356267.0000000004910000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000003.685637337.0000000000711000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000003.685637337.0000000000711000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000003.685637337.0000000000711000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D23CF06	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	6D23CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D215705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D21CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D215705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFA1B4F	ReadFile

Disassembly

Code Analysis