ID: 795911
Sample Name: nzCzLT1rR6.exe
Cookbook: default.jbs
Time: 13:16:10
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

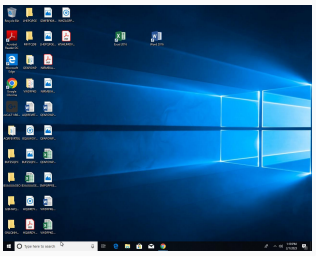
Windows Analysis Report

nzCzLT1rR6.exe

Overview

General Information

Sample Name:	nzCzLT1rR6.exe
Analysis ID:	795911
MD5:	2a4d85fb03059..
SHA1:	701232edaf6aa..
SHA256:	d7dc5a4583f40..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

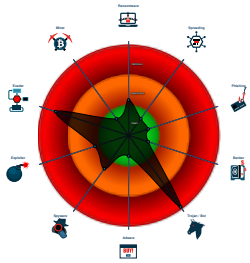
Nanocore, zgRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- nzCzLT1rR6.exe (PID: 6004 cmdline: C:\Users\user\Desktop\nzCzLT1rR6.exe MD5: 2A4D85FB030591CBFA42BBC72F27607E)
  - nzCzLT1rR6.exe (PID: 1216 cmdline: C:\Users\user\Desktop\nzCzLT1rR6.exe MD5: 2A4D85FB030591CBFA42BBC72F27607E)
    - schtasks.exe (PID: 3940 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp9373.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6036 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp9539.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nzCzLT1rR6.exe (PID: 6044 cmdline: C:\Users\user\Desktop\nzCzLT1rR6.exe 0 MD5: 2A4D85FB030591CBFA42BBC72F27607E)
  - nzCzLT1rR6.exe (PID: 5908 cmdline: C:\Users\user\Desktop\nzCzLT1rR6.exe MD5: 2A4D85FB030591CBFA42BBC72F27607E)
- dhcpmon.exe (PID: 1092 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2A4D85FB030591CBFA42BBC72F27607E)
  - dhcpmon.exe (PID: 2108 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 2A4D85FB030591CBFA42BBC72F27607E)
- dhcpmon.exe (PID: 5780 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2A4D85FB030591CBFA42BBC72F27607E)
  - dhcpmon.exe (PID: 5936 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 2A4D85FB030591CBFA42BBC72F27607E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "be28fce4-4930-4ffe-96ed-0110cf99",
  "Group": "SecureKMT",
  "Domain1": "tzitziklishop.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 1665,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x34e2:$x2: NanoCore.ClientPlugin • 0x350b:$x3: NanoCore.ClientPluginHost • 0x34d3:$i3: IClientNetwork • 0x34f8:$i6: IClientLoggingHost • 0x3525:$i7: IClientNetworkHost • 0x334e:$s1: ClientPlugin • 0x34eb:$s1: ClientPlugin
00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x350b:$a1: NanoCore.ClientPluginHost • 0x34e2:$a2: NanoCore.ClientPlugin • 0x5854:$b7: LogClientException • 0x34f8:$b9: IClientLoggingHost
00000012.00000002.333728253.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 102 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.nzCzLT1rR6.exe.3481c8c.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
1.2.nzCzLT1rR6.exe.3481c8c.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
1.2.nzCzLT1rR6.exe.3481c8c.2.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x6d7f:$x2: NanoCore.ClientPlugin • 0x6da5:$x3: NanoCore.ClientPluginHost • 0x6d70:$i3: IClientNetwork • 0x6d95:$i5: IClientDataHost • 0x6dbf:$i6: IClientLoggingHost • 0x6dd2:$i7: IClientNetworkHost • 0x6de5:$i9: IClientNameObjectCollection • 0x6b02:$s1: ClientPlugin • 0x6d88:$s1: ClientPlugin
1.2.nzCzLT1rR6.exe.3481c8c.2.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x6da5:$a1: NanoCore.ClientPluginHost • 0x6d7f:$a2: NanoCore.ClientPlugin • 0x6dbf:$b9: IClientLoggingHost
1.2.nzCzLT1rR6.exe.5016920.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 273 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26 −

Timestamp:	192.168.2.345.12.253.264970216652816766 02/01/23-13:18:00.977494
SID:	2816766
Source Port:	49702
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26 −

Timestamp:	192.168.2.345.12.253.264969816652816766 02/01/23-13:17:24.114380
SID:	2816766
Source Port:	49698
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.12.253.26 - Destination IP: 192.168.2.3 −

Timestamp:	45.12.253.26192.168.2.31665496982841753 02/01/23-13:17:23.356204
SID:	2841753
Source Port:	1665
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970016652025019 02/01/23-13:17:38.752931
SID:	2025019
Source Port:	49700
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.12.253.26 - Destination IP: 192.168.2.3

Timestamp:	45.12.253.26192.168.2.31665497002841753 02/01/23-13:17:43.786170
SID:	2841753
Source Port:	1665
Destination Port:	49700
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264971016652025019 02/01/23-13:18:53.106687
SID:	2025019
Source Port:	49710
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970116652816718 02/01/23-13:17:51.941680
SID:	2816718
Source Port:	49701
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.12.253.26 - Destination IP: 192.168.2.3

Timestamp:	45.12.253.26192.168.2.31665497012810290 02/01/23-13:17:50.835717
SID:	2810290
Source Port:	1665
Destination Port:	49701
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970916652816766 02/01/23-13:18:47.985288
SID:	2816766
Source Port:	49709
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970416652025019 02/01/23-13:18:12.511200
SID:	2025019
Source Port:	49704
Destination Port:	1665

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264970516652816766 02/01/23-13:18:21.103350
SID:	2816766
Source Port:	49705
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264971116652816766 02/01/23-13:19:05.431254
SID:	2816766
Source Port:	49711
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264969916652025019 02/01/23-13:17:29.785359
SID:	2025019
Source Port:	49699
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264971016652816718 02/01/23-13:18:54.276262
SID:	2816718
Source Port:	49710
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264970716652025019 02/01/23-13:18:33.167648
SID:	2025019
Source Port:	49707
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264970616652816766 02/01/23-13:18:27.570835
SID:	2816766
Source Port:	49706
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264970316652025019 02/01/23-13:18:06.200920
SID:	2025019
Source Port:	49703
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−

Timestamp:	192.168.2.345.12.253.264969816652025019 02/01/23-13:17:18.638360
SID:	2025019
Source Port:	49698
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970916652025019 02/01/23-13:18:47.017681
SID:	2025019
Source Port:	49709
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264971216652025019 02/01/23-13:19:24.159023
SID:	2025019
Source Port:	49712
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970616652025019 02/01/23-13:18:26.207894
SID:	2025019
Source Port:	49706
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970316652816766 02/01/23-13:18:07.370216
SID:	2816766
Source Port:	49703
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970716652816766 02/01/23-13:18:34.782616
SID:	2816766
Source Port:	49707
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970216652025019 02/01/23-13:17:57.465792
SID:	2025019
Source Port:	49702
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970816652816766 02/01/23-13:18:41.773314
SID:	2816766
Source Port:	49708
Destination Port:	1665

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.345.12.253.264970116652816766 02/01/23-13:17:51.941680
SID:	2816766
Source Port:	49701
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.345.12.253.264970816652025019 02/01/23-13:18:40.027997
SID:	2025019
Source Port:	49708
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.345.12.253.264969916652816766 02/01/23-13:17:30.963105
SID:	2816766
Source Port:	49699
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.345.12.253.264970016652816766 02/01/23-13:17:43.841016
SID:	2816766
Source Port:	49700
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.345.12.253.264971116652025019 02/01/23-13:19:04.505055
SID:	2025019
Source Port:	49711
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.345.12.253.264970516652025019 02/01/23-13:18:20.346491
SID:	2025019
Source Port:	49705
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.345.12.253.264970116652025019 02/01/23-13:17:50.278538
SID:	2025019
Source Port:	49701
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26

Timestamp:	192.168.2.345.12.253.264970416652816766 02/01/23-13:18:13.411136
SID:	2816766
Source Port:	49704
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.26	−
Timestamp:	192.168.2.345.12.253.264971016652816766 02/01/23-13:18:55.458400
SID:	2816766
Source Port:	49710
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected zgRAT

Yara detected Nanocore RAT

Remote Access Functionality

Yara detected zgRAT

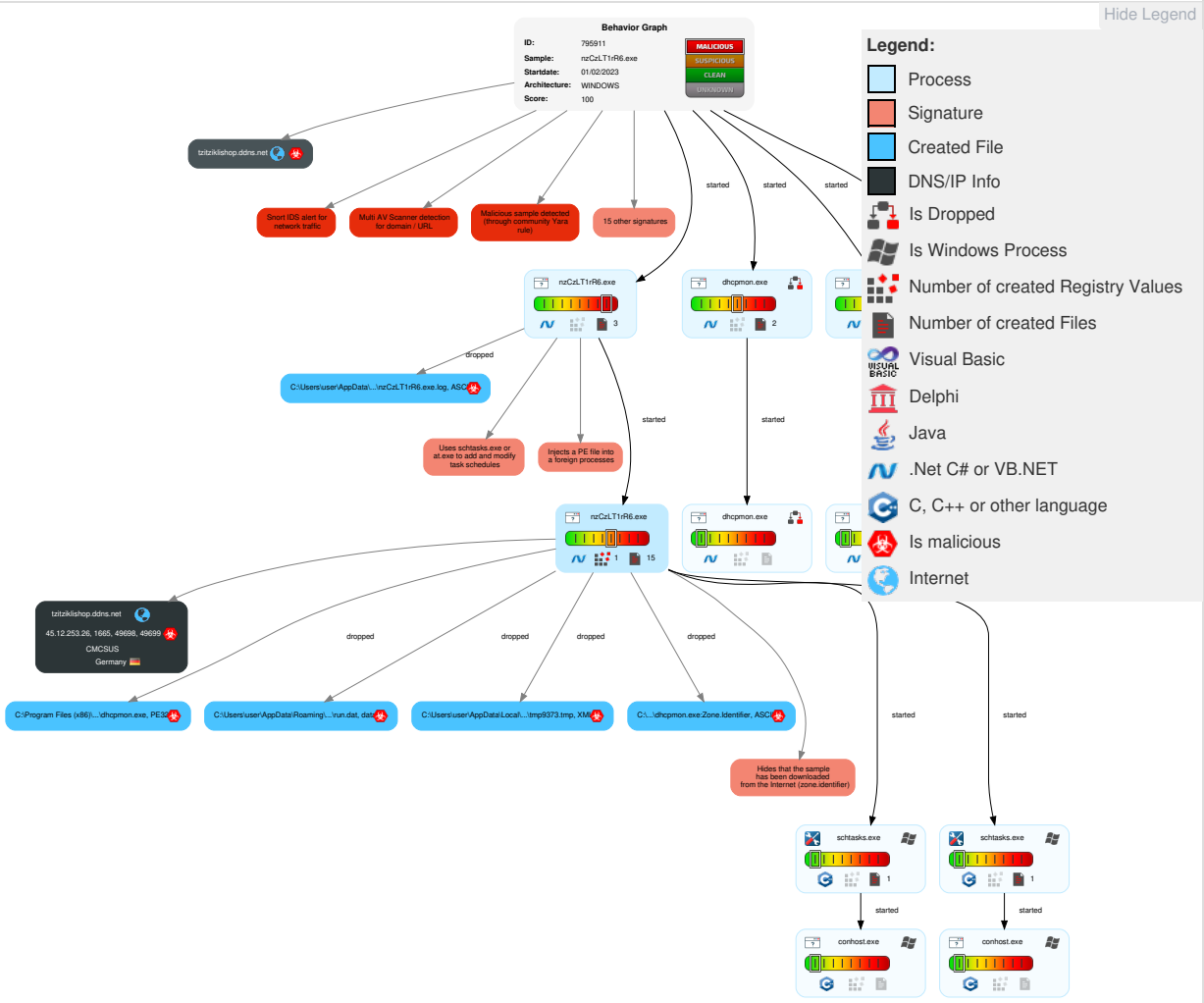
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	2 1 Input Capture	1 System Time Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 2 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nzCzLT1rR6.exe	28%	ReversingLabs		
nzCzLT1rR6.exe	30%	Virustotal		Browse
nzCzLT1rR6.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	28%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.nzCzLT1rR6.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.nzCzLT1rR6.exe.6970000.24.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
tzitziklishop.ddns.net	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
127.0.0.1	2%	Virustotal		Browse
tzitziklishop.ddns.net	12%	Virustotal		Browse
tzitziklishop.ddns.net	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	45.12.253.26	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
127.0.0.1	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

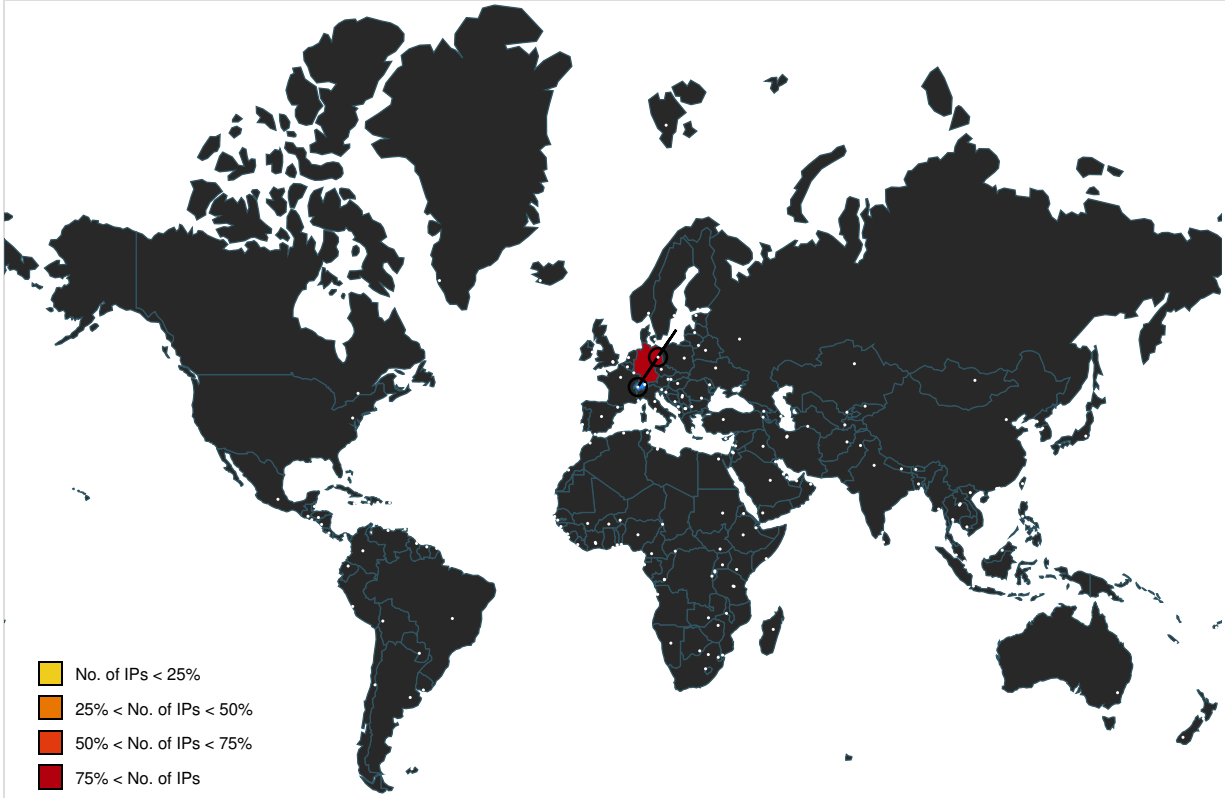
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	nzCzLT1rR6.exe, 00000001.00000002.530717785.0000000005011000.00000004.00000800.00020000.00000000.sdmp, nzCzLT1rR6.exe, 00000001.00000002.542851502.0000000007780000.00000004.08000000.00040000.00000000.sdmp, nzCzLT1rR6.exe, 00000001.00000002.530717785.0000000004CE0000.00000004.00000800.00020000.00000000.sdmp, nzCzLT1rR6.exe, 00000001.00000002.521288702.00000000033F1000.00000004.00000800.00020000.00000000.sdmp, nzCzLT1rR6.exe, 00000001.00000002.530717785.0000000004EB0000.00000004.00000800.00020000.00000000.sdmp, nzCzLT1rR6.exe, 00000001.00000002.530717785.0000000004F26000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	nzCzLT1rR6.exe, 00000001.00000002.521288702.00000000033F1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	nzCzLT1rR6.exe, 00000000.00000002.277951780.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.12.253.26	tzitziklishop.ddns.net	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	795911
Start date and time:	2023-02-01 13:16:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	nzCzLT1rR6.exe

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/11@15/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:17:11	API Interceptor	894x Sleep call for process: nzCzLT1rR6.exe modified
13:17:15	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\nzCzLT1rR6.exe" s>$(Arg0)
13:17:16	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:17:17	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
13:17:27	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe

File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	856064
Entropy (8bit):	7.392672284816359
Encrypted:	false
SSDEEP:	24576:peia1r8NO9c1xqpB9cbOEx54w6RTc4N34HZ:ps1r8M9WmzcbOEbKE
MD5:	2A4D85FB030591CBFA42BBC72F27607E
SHA1:	701232EDAF6AA4A36509644D69B6A7C55443B1B6
SHA-256:	D7DC5A4583F409639BF8C10EB62FBBC13AC2E1B8F702425E959D47E64463D45F
SHA-512:	4E17DEF1C104C95BC784B58DD0B1445050D3489225F27C60EC0253AF302F44E04DA25C3743606865F85D1940A4EF3B90ED50D58B98ED0A0CCC21A39366A4A4E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5.c.....0.....(..... .....@.. .....@..... ..@.....O..... .....T..... ....H.....text...T.... ....`.rsrc..... .....@..@.reloc..... .....@..B..... .....

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

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
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:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nzCzLT1rR6.exe.log

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp9373.tmp

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.1134186573278635
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK02xtn:cbk4oL600QydbQxIYODOLedq3Bj
MD5:	EA0A9B3D723EFB29247BFCC232623350
SHA1:	2B2A2216A879A594F446C62A7DF5BBAE40EA2F34
SHA-256:	D35E198665E7BB3750E00F867B7579075720D38926062CB7362E1E912FE29B54
SHA-512:	81D5AFA7D63D0D6B8754A029B2D6FCF4E854CDC295B84E4B56AEEFB9643FFC157CA1C2C4B73813C67788FC2FD9DA2CE0A6AAD17A65AEC4482A5D21D9C714484
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\tmp9539.tmp

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	data

Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:l+t:lS
MD5:	22308B91A420C8005645AD61D0EFA476
SHA1:	E4D0F227DA23E59AAF838155C79B4BF60BCA6A70
SHA-256:	22A68CB21E4FA5445DEAC968EC01AED2305C1C629C076275F963BFE393512C43
SHA-512:	9222A796A7E7C6E9410D7DDE631159E4D9228079273A364D7432B79EE4E04934BBD7FFCC79BFAEAE2C5E104AEE95A24180D7FA03C3ED73C2F8C67553CE5C1D68
Malicious:	**true**
Preview:	......H

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

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

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

Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPlZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926
Malicious:	false

Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v.""..v.......#..X.a...../...cC...i..l{>5n.._+.e.d'...}....[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\nzCzLT1rR6.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.337435460048129
Encrypted:	false
SSDEEP:	3:oNWXp5vLcx5Cn:oNWXpFscn
MD5:	EAF8F534247E1E2C45FE31206C50AF6E
SHA1:	2C7FD6E43C9F8F9A1E81BF028A97D25A2E146228
SHA-256:	F52465571F68F951E008AADCB47E29588FEAF9BB4D0E5941F8A6322BBB224243
SHA-512:	A4D98BACF3DF8D0348274C9ECC8BE155EEA58AE635300929C4F7E08B2A2FC782674A0C9C1A03BAEB015513E94CFCC267BE0C1B0D2FF9EFA937AA1057EE7DE 685
Malicious:	false
Preview:	C:\Users\user\Desktop\nzCzLT1rR6.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.392672284816359
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	nzCzLT1rR6.exe
File size:	856064
MD5:	2a4d85fb030591cbfa42bbc72f27607e
SHA1:	701232edaf6aa4a36509644d69b6a7c55443b1b6
SHA256:	d7dc5a4583f409639bf8c10eb62fbbc13ac2e1b8f702425e959d47e64463d45f
SHA512:	4e17def1c104c95bc784b58dd0b1445050d3489225f27c60ec0253af302f44e04da25c3743606865f85d1940a4ef3b90ed50d58b98ed0a0ccc21a39366a4a4e8
SSDEEP:	24576:peia1r8NO9c1xqpB9cbOEx54w6RTc4N34HZ:ps1r8M9WmzcbOEbKE
TLSH:	40056A8137B15862F1DB05B91028778C1E3D7443A6E6E2665BBB39C49703AF7F298F12
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5.c.....0.....(..... .....@.. .....@.....@.....

File Icon

Icon Hash:	821de22b2b661982

Static PE Info

General

Entrypoint:	0x4cfb0e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63DA35FD [Wed Feb 1 09:50:53 2023 UTC]

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcfabc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0x1904	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0xcbeb0	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcdc54	0xce000	False	0.7378640776699029	data	7.413609935503911	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x1904	0x2000	False	0.6446533203125	data	6.110407966825619	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x800	False	0.015625	data	0.02939680787012526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd0100	0x1296	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xd13a8	0x14	data		
RT_VERSION	0xd13cc	0x338	data		
RT_MANIFEST	0xd1714	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

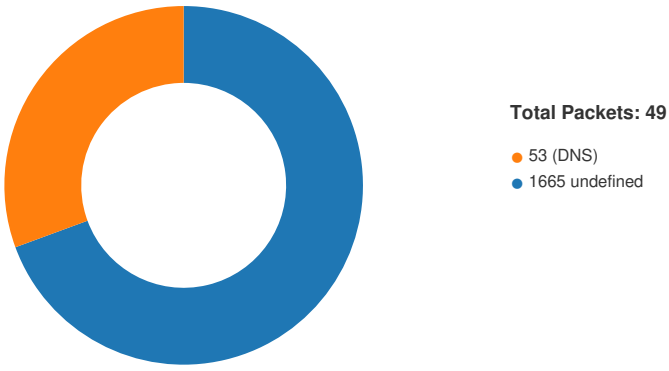
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.12.253.264970216652816766 02/01/23-13:18:00.977494	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264969816652816766 02/01/23-13:17:24.114380	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49698	1665	192.168.2.3	45.12.253.26
45.12.253.26192.168.2.31665496982841753 02/01/23-13:17:23.356204	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1665	49698	45.12.253.26	192.168.2.3
192.168.2.345.12.253.264970016652025019 02/01/23-13:17:38.752931	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	1665	192.168.2.3	45.12.253.26
45.12.253.26192.168.2.31665497002841753 02/01/23-13:17:43.786170	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1665	49700	45.12.253.26	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.12.253.264 971016652025019 02/01/23-13:18:53.106687	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970116652816718 02/01/23-13:17:51.941680	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49701	1665	192.168.2.3	45.12.253.26
45.12.253.26192.168.2.31 665497012810290 02/01/23-13:17:50.835717	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1665	49701	45.12.253.26	192.168.2.3
192.168.2.345.12.253.264 970916652816766 02/01/23-13:18:47.985288	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970416652025019 02/01/23-13:18:12.511200	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970516652816766 02/01/23-13:18:21.103350	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 971116652816766 02/01/23-13:19:05.431254	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 969916652025019 02/01/23-13:17:29.785359	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 971016652816718 02/01/23-13:18:54.276262	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49710	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970716652025019 02/01/23-13:18:33.167648	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970616652816766 02/01/23-13:18:27.570835	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970316652025019 02/01/23-13:18:06.200920	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 969816652025019 02/01/23-13:17:18.638360	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970916652025019 02/01/23-13:18:47.017681	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 971216652025019 02/01/23-13:19:24.159023	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970616652025019 02/01/23-13:18:26.207894	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970316652816766 02/01/23-13:18:07.370216	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970716652816766 02/01/23-13:18:34.782616	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970216652025019 02/01/23-13:17:57.465792	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	1665	192.168.2.3	45.12.253.26

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.12.253.264 970816652816766 02/01/23-13:18:41.773314	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970116652816766 02/01/23-13:17:51.941680	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970816652025019 02/01/23-13:18:40.027997	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 969916652816766 02/01/23-13:17:30.963105	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49699	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970016652816766 02/01/23-13:17:43.841016	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49700	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 971116652025019 02/01/23-13:19:04.505055	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970516652025019 02/01/23-13:18:20.346491	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970116652025019 02/01/23-13:17:50.278538	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 970416652816766 02/01/23-13:18:13.411136	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	1665	192.168.2.3	45.12.253.26
192.168.2.345.12.253.264 971016652816766 02/01/23-13:18:55.458400	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	1665	192.168.2.3	45.12.253.26

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 13:17:18.288016081 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:18.314538002 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:18.314672947 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:18.638360023 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:18.723278999 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:18.791244030 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:18.838916063 CET	49698	1665	192.168.2.3	45.12.253.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 13:17:18.869852066 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:18.964178085 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:18.966751099 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.051708937 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.051852942 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.134402990 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.219264984 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.219301939 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.219322920 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.219341993 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.219381094 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.219430923 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.246212959 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246263027 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246283054 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246303082 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246323109 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246340990 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246354103 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.246364117 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246383905 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.246423960 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.246464014 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.272747993 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273128986 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273154974 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273175001 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273195028 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273202896 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.273216009 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273237944 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273257971 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273258924 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.273278952 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273298979 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273309946 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.273319960 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273339987 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273343086 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.273360968 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273380995 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273396015 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.273401976 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.273433924 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.299825907 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.299870968 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.299891949 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.299900055 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.299912930 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.299932957 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.299940109 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.299954891 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.299973965 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.299990892 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.299995899 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300019026 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300038099 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300045013 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300060034 CET	1665	49698	45.12.253.26	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 13:17:19.300080061 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300081968 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300101042 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300105095 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300122023 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300141096 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300144911 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300159931 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300179958 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300194025 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300199986 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300219059 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300223112 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300240040 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300260067 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300262928 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300281048 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300299883 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300304890 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300319910 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300343990 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300487995 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300508022 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300542116 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300543070 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.300576925 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.300580025 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.330279112 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.330310106 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.330327988 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.330336094 CET	49698	1665	192.168.2.3	45.12.253.26
Feb 1, 2023 13:17:19.330349922 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.330370903 CET	1665	49698	45.12.253.26	192.168.2.3
Feb 1, 2023 13:17:19.330374002 CET	49698	1665	192.168.2.3	45.12.253.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 13:17:18.230256081 CET	62704	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:17:18.249610901 CET	53	62704	8.8.8.8	192.168.2.3
Feb 1, 2023 13:17:29.726079941 CET	49977	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:17:29.747073889 CET	53	49977	8.8.8.8	192.168.2.3
Feb 1, 2023 13:17:38.681685925 CET	57840	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:17:38.699248075 CET	53	57840	8.8.8.8	192.168.2.3
Feb 1, 2023 13:17:50.227096081 CET	57990	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:17:50.248939037 CET	53	57990	8.8.8.8	192.168.2.3
Feb 1, 2023 13:17:57.084634066 CET	52387	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:17:57.106492043 CET	53	52387	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:06.151191950 CET	56924	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:18:06.172343969 CET	53	56924	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:12.388278008 CET	60625	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:18:12.405318022 CET	53	60625	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:20.170303106 CET	49302	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:18:20.192081928 CET	53	49302	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:26.153378010 CET	53975	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:18:26.172627926 CET	53	53975	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:33.111686945 CET	51139	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:18:33.131355047 CET	53	51139	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:39.978817940 CET	52955	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 13:18:39.998919964 CET	53	52955	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:46.957595110 CET	60582	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:18:46.976948977 CET	53	60582	8.8.8.8	192.168.2.3
Feb 1, 2023 13:18:52.987720966 CET	57134	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:18:53.006586075 CET	53	57134	8.8.8.8	192.168.2.3
Feb 1, 2023 13:19:01.442071915 CET	62050	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:19:01.463848114 CET	53	62050	8.8.8.8	192.168.2.3
Feb 1, 2023 13:19:24.105247021 CET	56042	53	192.168.2.3	8.8.8.8
Feb 1, 2023 13:19:24.127202988 CET	53	56042	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 13:17:18.230256081 CET	192.168.2.3	8.8.8.8	0x6d87	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:29.726079941 CET	192.168.2.3	8.8.8.8	0x7808	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:38.681685925 CET	192.168.2.3	8.8.8.8	0xf922	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:50.227096081 CET	192.168.2.3	8.8.8.8	0x329d	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:57.084634066 CET	192.168.2.3	8.8.8.8	0x6528	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:06.151191950 CET	192.168.2.3	8.8.8.8	0x3dea	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:12.388278008 CET	192.168.2.3	8.8.8.8	0x3ac6	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:20.170303106 CET	192.168.2.3	8.8.8.8	0x7fbd	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:26.153378010 CET	192.168.2.3	8.8.8.8	0xbf46	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:33.111686945 CET	192.168.2.3	8.8.8.8	0x8d01	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:39.978817940 CET	192.168.2.3	8.8.8.8	0x4935	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:46.957595110 CET	192.168.2.3	8.8.8.8	0xcb3	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:52.987720966 CET	192.168.2.3	8.8.8.8	0x1672	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:19:01.442071915 CET	192.168.2.3	8.8.8.8	0xa7f2	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:19:24.105247021 CET	192.168.2.3	8.8.8.8	0xf687	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false

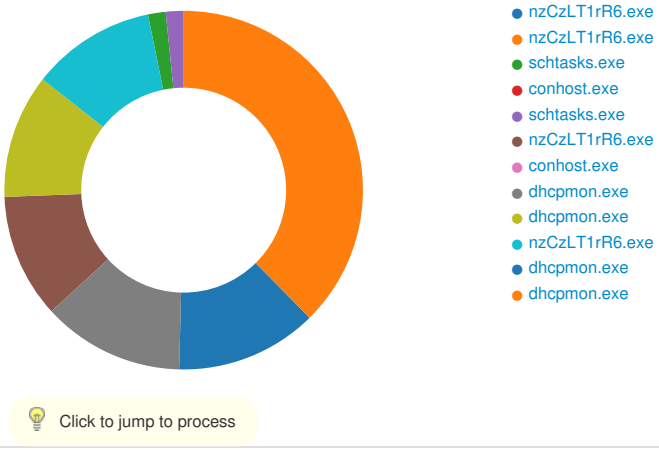
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 13:17:18.249610901 CET	8.8.8.8	192.168.2.3	0x6d87	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:29.747073889 CET	8.8.8.8	192.168.2.3	0x7808	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:38.699248075 CET	8.8.8.8	192.168.2.3	0xf922	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:50.248939037 CET	8.8.8.8	192.168.2.3	0x329d	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:17:57.106492043 CET	8.8.8.8	192.168.2.3	0x6528	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:06.172343969 CET	8.8.8.8	192.168.2.3	0x3dea	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:12.405318022 CET	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 13:18:20.192081928 CET	8.8.8.8	192.168.2.3	0x7fbd	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:26.172627926 CET	8.8.8.8	192.168.2.3	0xbf46	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:33.131355047 CET	8.8.8.8	192.168.2.3	0x8d01	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:39.998919964 CET	8.8.8.8	192.168.2.3	0x4935	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:46.976948977 CET	8.8.8.8	192.168.2.3	0xcb3	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:18:53.006586075 CET	8.8.8.8	192.168.2.3	0x1672	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:19:01.463848114 CET	8.8.8.8	192.168.2.3	0xa7f2	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 13:19:24.127202988 CET	8.8.8.8	192.168.2.3	0xf687	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: nzCzLT1rR6.exe PID: **6004**, Parent PID: **3452**

General

Target ID:	0
Start time:	13:17:05
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\nzCzLT1rR6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\nzCzLT1rR6.exe
Imagebase:	0x770000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.269552215.0000000003C6C000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.269552215.0000000003C6C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.269552215.0000000003C6C000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.269552215.0000000003C6C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.267300740.0000000002C64000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nzCzLT1rR6.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	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\nzCzLT1rR6.exe.log	0	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: nzCzLT1rR6.exe PID: **1216**, Parent PID: **6004**

General

Target ID:	1
Start time:	13:17:12
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\nzCzLT1rR6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\nzCzLT1rR6.exe
Imagebase:	0xf60000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E
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: 00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.543241972.00000000077C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.543793463.0000000007950000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.543793463.0000000007950000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.543793463.0000000007950000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.543793463.0000000007950000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.543011972.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.543011972.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.543011972.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.543011972.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.540605869.00000000066F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.540605869.00000000066F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.540605869.00000000066F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.540605869.00000000066F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.539921982.0000000005E40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.539921982.0000000005E40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.539921982.0000000005E40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.539921982.0000000005E40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.540271148.00000000066B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.540271148.00000000066B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.540271148.00000000066B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.540271148.00000000066B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.542851502.0000000007780000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.542851502.0000000007780000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.542851502.0000000007780000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.542851502.0000000007780000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.540954705.0000000006970000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.540954705.0000000006970000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.540954705.0000000006970000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.540954705.0000000006970000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.540954705.0000000006970000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.540194138.00000000066A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.540194138.00000000066A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.540194138.00000000066A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.540194138.00000000066A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000003.287933444.0000000006D26000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.530717785.0000000005011000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000002.530717785.0000000005011000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.530717785.0000000005011000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.542239209.0000000006E20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.542239209.0000000006E20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.542239209.0000000006E20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.542239209.0000000006E20000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.540666148.0000000006700000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.540666148.0000000006700000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.540666148.0000000006700000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.540666148.0000000006700000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.530717785.0000000004EB0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000002.530717785.0000000004EB0000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.530717785.0000000004EB0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.542942575.0000000007790000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.542942575.0000000007790000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.542942575.0000000007790000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.542942575.0000000007790000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.540745789.0000000006710000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.540745789.0000000006710000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.540745789.0000000006710000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.540745789.0000000006710000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.530717785.0000000004CE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000002.530717785.0000000004CE0000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.530717785.0000000004CE0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000001.00000002.530717785.0000000004F26000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.530717785.0000000004F26000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.521288702.000000000033F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000002.521288702.000000000033F1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.521288702.00000000033F1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.543341019.00000000077D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.543341019.00000000077D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.543341019.00000000077D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.543341019.00000000077D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	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	717EBEFF	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	717E1E60	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	717EBEFF	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	717EDD66	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	717EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9373.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	717E7038	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	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp9539.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	717E7038	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	717EBEFF	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	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	10	717E1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9373.tmp	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9539.tmp	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\Desktop\nzCzLT1rR6.exe:Zone.Identifier	success or wait	1	71762935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd fd 30 fd 04 fd 48	H	success or wait	1	717E1B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 35 fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 28 00 00 00 00 00 00 0e fd 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 08 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0d 00 00 08 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL5c0(@ @@	success or wait	4	717EDD66	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	717EDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9373.tmp	0	1300	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	717E1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	37	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 6e 7a 43 7a 4c 54 31 72 52 36 2e 65 78 65	C:\Users\user\Desktop\nzCzLT1rR6.exe	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp9539.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	14	717E1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 16 fd fd 20 38 fd 6a fd fd fd fd 7c fd 26 58 fd fd 65 fd 46 fd 2a fd	9iH}Z4f 8j|&XeF*	success or wait	1	717E1B4F	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7295D72F	unknown
C:\Users\user\Desktop\nzCzLT1rR6.exe	unknown	4096	success or wait	1	7295D72F	unknown
C:\Users\user\Desktop\nzCzLT1rR6.exe	unknown	512	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7295D72F	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	717E646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **3940**, Parent PID: **1216**

General

Target ID:	2
Start time:	13:17:14
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp9373.tmp
Imagebase:	0x1260000
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\tmp9373.tmp	unknown	2	success or wait	1	126AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9373.tmp	unknown	1301	success or wait	1	126ABD9	ReadFile

Analysis Process: conhost.exe PID: **4696**, Parent PID: **3940**

General

Target ID:	3
Start time:	13:17:14
Start date:	01/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **6036**, Parent PID: **1216**

General

Target ID:	4
Start time:	13:17:15
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp9539.tmp
Imagebase:	0x1260000
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\tmp9539.tmp	unknown	2	success or wait	1	126AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9539.tmp	unknown	1311	success or wait	1	126ABD9	ReadFile

Analysis Process: nzCzLT1rR6.exe PID: **6044**, Parent PID: **1080**

General

Target ID:	5
Start time:	13:17:15
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\nzCzLT1rR6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\nzCzLT1rR6.exe 0
Imagebase:	0x3d0000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **6008**, Parent PID: **6036**

General

Target ID:	6
Start time:	13:17:15
Start date:	01/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: dhcpmon.exe PID: **1092**, Parent PID: **1080**

General

Target ID:	7
Start time:	13:17:17
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x490000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.313319799.00000000029F4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	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	72CAC78D	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	0	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile

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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **5780**, Parent PID: **3452**

General

Target ID:	10
Start time:	13:17:24
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x950000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: nzCzLT1rR6.exe PID: **5908**, Parent PID: **6044**

General

Target ID:	18
Start time:	13:17:28
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\nzCzLT1rR6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\nzCzLT1rR6.exe
Imagebase:	0x840000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E
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: 00000012.00000002.333728253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.333728253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.333728253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000012.00000002.333728253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.341628042.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.341628042.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000012.00000002.341628042.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.343896374.0000000003BE9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.343896374.0000000003BE9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000012.00000002.343896374.0000000003BE9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **2108**, Parent PID: **1092**

General	
Target ID:	19
Start time:	13:17:32
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xd50000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.347590788.0000000003231000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.347590788.0000000003231000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.347590788.0000000003231000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: dhcpmon.exe PID: **5936**, Parent PID: **5780**

General	
Target ID:	20
Start time:	13:17:42
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xd20000
File size:	856064 bytes
MD5 hash:	2A4D85FB030591CBFA42BBC72F27607E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Disassembly

No disassembly