ID: 878777
Sample Name:
SAaX2wNRn2.exe
Cookbook: default.jbs
Time: 07:51:06
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

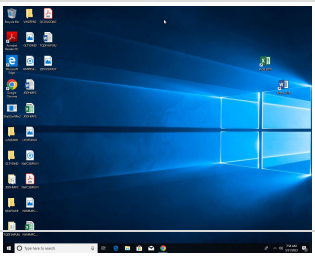
Windows Analysis Report

SAaX2wNRn2.exe

Overview

General Information

Sample Name:	SAaX2wNRn2.exe
Original Sample Name:	e89323dd0063…
Analysis ID:	878777
MD5:	e89323dd0063…
SHA1:	788e5fcae9e19..
SHA256:	70d856cfc4e27..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

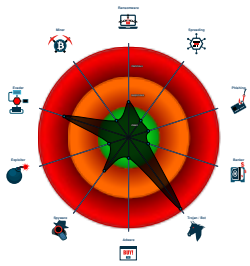
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- SAaX2wNRn2.exe (PID: 2152 cmdline: C:\Users\user\Desktop\SAaX2wNRn2.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
  - SAaX2wNRn2.exe (PID: 2888 cmdline: C:\Users\user\Desktop\SAaX2wNRn2.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
    - schtasks.exe (PID: 5312 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp1C83.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5744 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp1E68.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SAaX2wNRn2.exe (PID: 2244 cmdline: C:\Users\user\Desktop\SAaX2wNRn2.exe 0 MD5: E89323DD0063FB87B2115AF014BBAF94)
    - SAaX2wNRn2.exe (PID: 6852 cmdline: C:\Users\user\Desktop\SAaX2wNRn2.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
    - SAaX2wNRn2.exe (PID: 5708 cmdline: C:\Users\user\Desktop\SAaX2wNRn2.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
    - SAaX2wNRn2.exe (PID: 6840 cmdline: C:\Users\user\Desktop\SAaX2wNRn2.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
- dhcpmon.exe (PID: 2844 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: E89323DD0063FB87B2115AF014BBAF94)
  - dhcpmon.exe (PID: 6744 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
  - dhcpmon.exe (PID: 5788 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
- dhcpmon.exe (PID: 4984 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: E89323DD0063FB87B2115AF014BBAF94)
  - dhcpmon.exe (PID: 3712 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E89323DD0063FB87B2115AF014BBAF94)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	http://https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "540c4d56-ad4d-4ca4-9f9f-305dba1d",
  "Group": "Default",
  "Domain1": "jasonbourneblack.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 4032,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x5b0b:$x2: NanoCore.ClientPluginHost • 0x5c0f:$s4: PipeCreated • 0x5b25:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x5b87:$x2: NanoCore.ClientPlugin • 0x5b0b:$x3: NanoCore.ClientPluginHost • 0x5b9d:$i3: IClientNetwork • 0x5b25:$i6: IClientLoggingHost • 0x5b44:$i7: IClientNetworkHost • 0x57fb:$s1: ClientPlugin • 0x5b90:$s1: ClientPlugin • 0x6cf4:$s3: IPAddress
00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x5b0b:$a1: NanoCore.ClientPluginHost • 0x5b87:$a2: NanoCore.ClientPlugin • 0x6710:$b7: LogClientException • 0x5b25:$b9: IClientLoggingHost
00000001.00000002.672248267.0000000003BFD000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x55d87:$a: NanoCore • 0x55e71:$a: NanoCore • 0x56ce8:$a: NanoCore • 0x5fe92:$a: NanoCore • 0x5fef3:$a: NanoCore • 0x5ff36:$a: NanoCore • 0x5ff76:$a: NanoCore • 0x601b2:$a: NanoCore • 0x60252:$a: NanoCore • 0x60a2a:$a: NanoCore • 0x6101d:$a: NanoCore • 0x6116e:$a: NanoCore • 0x61fc8:$a: NanoCore • 0x6222f:$a: NanoCore • 0x62244:$a: NanoCore • 0x62263:$a: NanoCore • 0x6b166:$a: NanoCore • 0x6b18f:$a: NanoCore • 0x76f08:$a: NanoCore • 0x76f31:$a: NanoCore • 0x9bdf4:$a: NanoCore
Click to see the 94 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.SAaX2wNRn2.exe.3c597c7.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1deb:$x1: NanoCore.ClientPluginHost • 0x1e24:$x2: IClientNetworkHost
1.2.SAaX2wNRn2.exe.3c597c7.12.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1deb:$x2: NanoCore.ClientPluginHost • 0x1f36:$s4: PipeCreated • 0x1e05:$s5: IClientLoggingHost
1.2.SAaX2wNRn2.exe.3c597c7.12.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x1e8b:$x2: NanoCore.ClientPlugin • 0x1deb:$x3: NanoCore.ClientPluginHost • 0x1ea1:$i3: IClientNetwork • 0x1e43:$i5: IClientDataHost • 0x1e05:$i6: IClientLoggingHost • 0x1e24:$i7: IClientNetworkHost • 0x266c:$i9: IClientNameObjectCollection • 0x1b41:$s1: ClientPlugin • 0x1e94:$s1: ClientPlugin • 0x2a80:$s2: EndPoint • 0x2771:$s3: IPAddress • 0x2083:$s4: IPEndPoint • 0x27a3:$s7: get_Connected
1.2.SAaX2wNRn2.exe.3c597c7.12.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x1deb:$a1: NanoCore.ClientPluginHost • 0x1e8b:$a2: NanoCore.ClientPlugin • 0x2be1:$b7: LogClientException • 0x1e05:$b9: IClientLoggingHost
1.2.SAaX2wNRn2.exe.6bb0000.27.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
Click to see the 265 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: 192.168.2.5 - Destination IP: 141.98.6.167

Timestamp:	192.168.2.5141.98.6.1674972340322816766 05/31/23-07:53:03.283583
SID:	2816766
Source Port:	49723
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167

Timestamp:	192.168.2.5141.98.6.1674971640322816766 05/31/23-07:52:13.461105
SID:	2816766
Source Port:	49716
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167

Timestamp:	192.168.2.5141.98.6.1674971840322025019 05/31/23-07:52:31.617417
SID:	2025019
Source Port:	49718
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167

Timestamp:	192.168.2.5141.98.6.1674972840322025019 05/31/23-07:53:33.869411
SID:	2025019
Source Port:	49728
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167

Timestamp:	192.168.2.5141.98.6.1674972940322816766 05/31/23-07:53:43.288922
SID:	2816766
Source Port:	49729
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167

Timestamp:	192.168.2.5141.98.6.1674973340322816766 05/31/23-07:54:08.525317

SID:	2816766
Source Port:	49733
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674973240322025019 05/31/23-07:54:01.126019
SID:	2025019
Source Port:	49732
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674971940322816766 05/31/23-07:52:40.572861
SID:	2816766
Source Port:	49719
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674971940322025019 05/31/23-07:52:39.496237
SID:	2025019
Source Port:	49719
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972240322025019 05/31/23-07:52:54.172177
SID:	2025019
Source Port:	49722
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674973040322816766 05/31/23-07:53:49.430104
SID:	2816766
Source Port:	49730
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 141.98.6.167 - Destination IP: 192.168.2.5	
Timestamp:	141.98.6.167192.168.2.54032497182810290 05/31/23-07:52:32.211435
SID:	2810290
Source Port:	4032
Destination Port:	49718
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674973240322816718 05/31/23-07:54:02.704983
SID:	2816718
Source Port:	49732
Destination Port:	4032
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674971640322025019 05/31/23-07:52:11.267334
SID:	2025019
Source Port:	49716
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972040322816766 05/31/23-07:52:48.788255
SID:	2816766
Source Port:	49720
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972440322816766 05/31/23-07:53:09.525595
SID:	2816766
Source Port:	49724
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972540322025019 05/31/23-07:53:15.239239
SID:	2025019
Source Port:	49725
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674973140322025019 05/31/23-07:53:54.566547
SID:	2025019
Source Port:	49731
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972940322025019 05/31/23-07:53:42.302533
SID:	2025019
Source Port:	49729
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674973140322816766 05/31/23-07:53:56.008756
SID:	2816766
Source Port:	49731
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674971840322816766 05/31/23-07:52:32.730530

SID:	2816766
Source Port:	49718
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674972840322816766 05/31/23-07:53:36.859358
SID:	2816766
Source Port:	49728
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674972340322025019 05/31/23-07:53:02.033758
SID:	2025019
Source Port:	49723
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 141.98.6.167 - Destination IP: 192.168.2.5	−
Timestamp:	141.98.6.167192.168.2.54032497332841753 05/31/23-07:54:23.318530
SID:	2841753
Source Port:	4032
Destination Port:	49733
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674972040322025019 05/31/23-07:52:47.324081
SID:	2025019
Source Port:	49720
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674972640322025019 05/31/23-07:53:20.721069
SID:	2025019
Source Port:	49726
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674973040322025019 05/31/23-07:53:48.374058
SID:	2025019
Source Port:	49730
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 141.98.6.167 - Destination IP: 192.168.2.5	−
Timestamp:	141.98.6.167192.168.2.54032497252841753 05/31/23-07:53:15.269919
SID:	2841753
Source Port:	4032
Destination Port:	49725
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 141.98.6.167 - Destination IP: 192.168.2.5	
Timestamp:	141.98.6.167192.168.2.54032497172841753 05/31/23-07:52:25.058340
SID:	2841753
Source Port:	4032
Destination Port:	49717
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972240322816766 05/31/23-07:52:55.998811
SID:	2816766
Source Port:	49722
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972440322025019 05/31/23-07:53:08.375676
SID:	2025019
Source Port:	49724
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972740322816766 05/31/23-07:53:28.901780
SID:	2816766
Source Port:	49727
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674971740322816766 05/31/23-07:52:22.187780
SID:	2816766
Source Port:	49717
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674971740322025019 05/31/23-07:52:20.026839
SID:	2025019
Source Port:	49717
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972640322816766 05/31/23-07:53:21.715954
SID:	2816766
Source Port:	49726
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	
Timestamp:	192.168.2.5141.98.6.1674972040322816718 05/31/23-07:52:47.571898

SID:	2816718
Source Port:	49720
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674973240322816766 05/31/23-07:54:02.704983
SID:	2816766
Source Port:	49732
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674972740322025019 05/31/23-07:53:27.404072
SID:	2025019
Source Port:	49727
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 141.98.6.167	−
Timestamp:	192.168.2.5141.98.6.1674973340322025019 05/31/23-07:54:08.288405
SID:	2025019
Source Port:	49733
Destination Port:	4032
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- 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)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

Yara detected Nanocore RAT

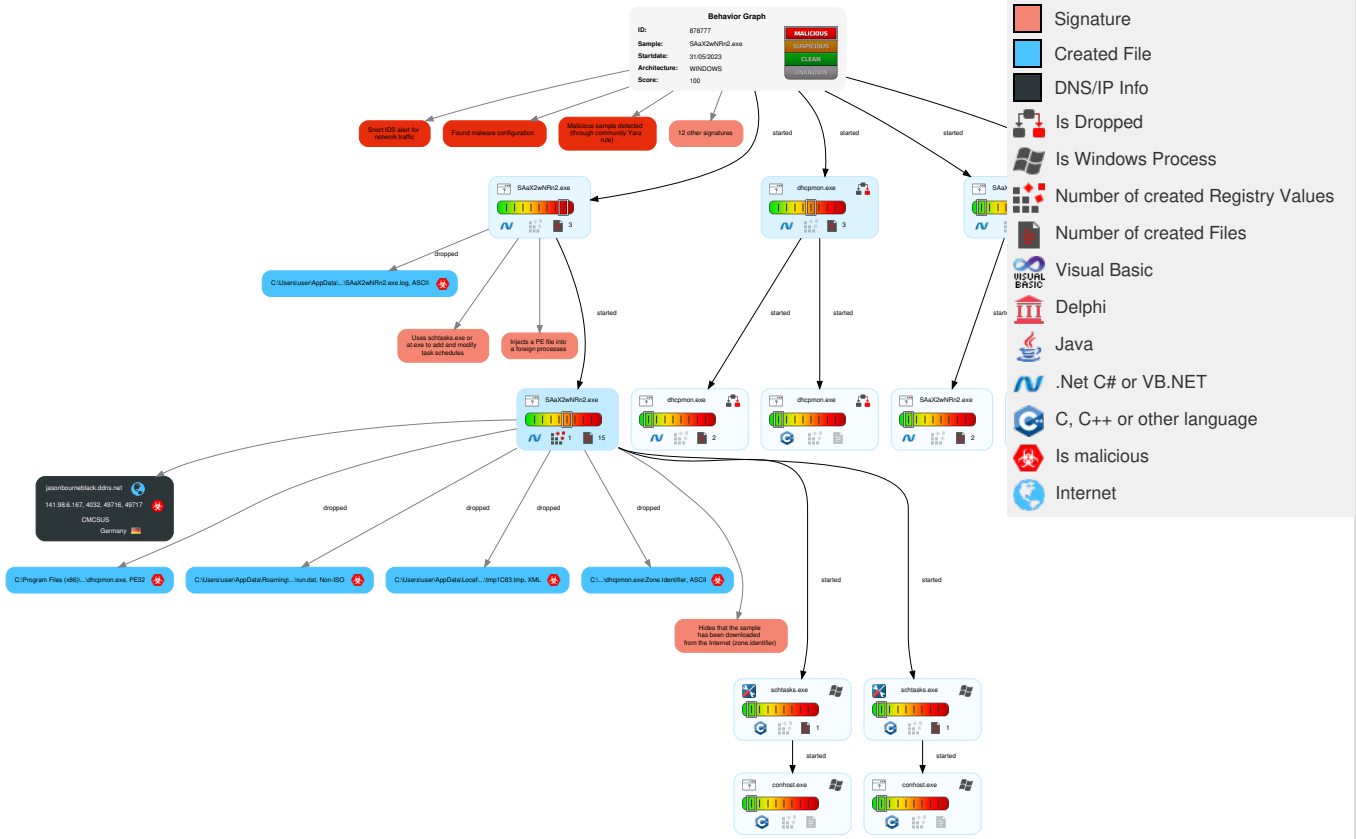
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	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	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 1 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	At (Linux)	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	2 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

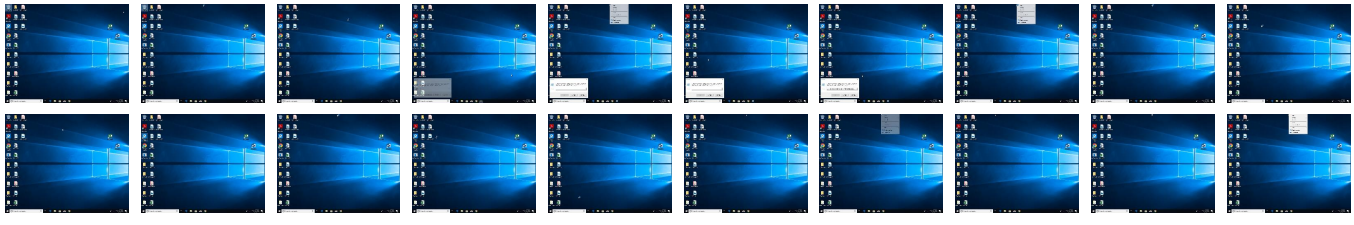
Hide Legend



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
SAaX2wNRn2.exe	38%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
SAaX2wNRn2.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	38%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
127.0.0.1	0%	Avira URL Cloud	safe	
jasonbourneblack.ddns.net	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jasonbourneblack.ddns.net	141.98.6.167	true	true		unknown

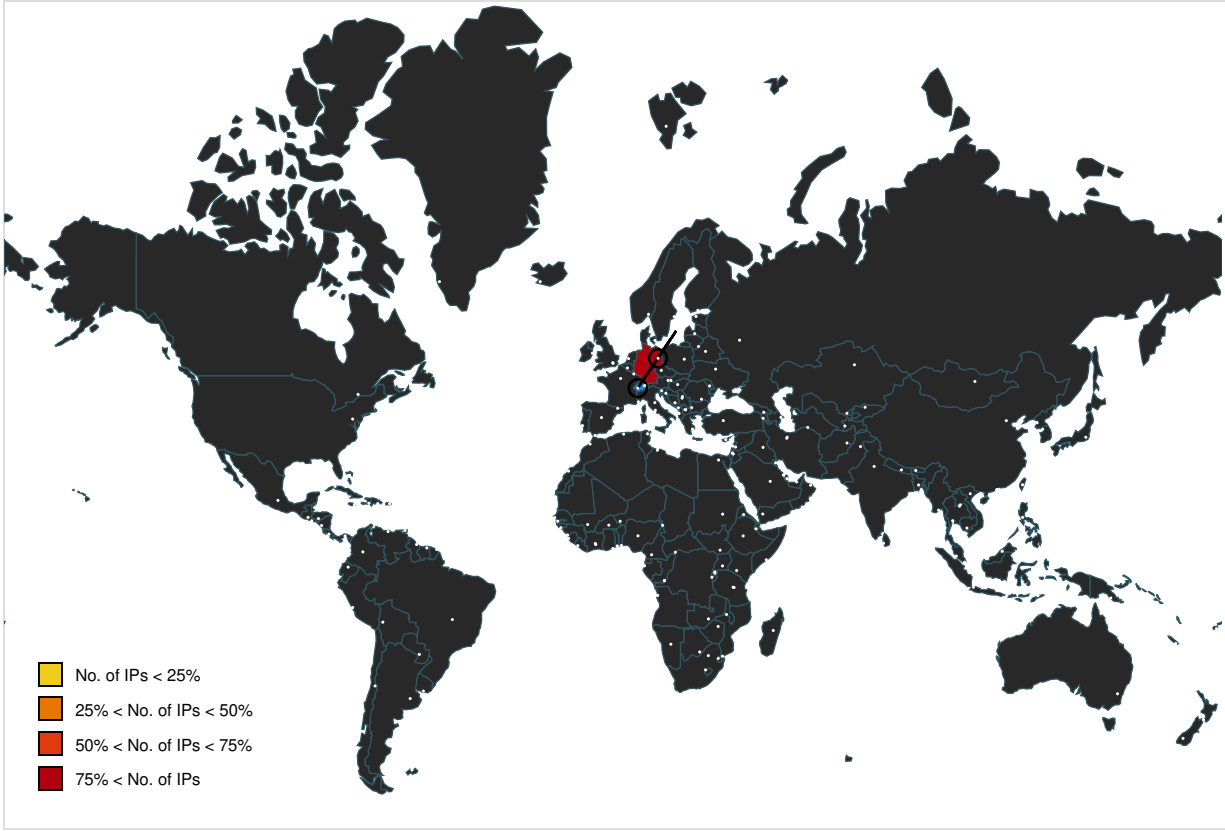
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
jasonbourneblack.ddns.net	true	• Avira URL Cloud: malware	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	SAaX2wNRn2.exe, 00000001.00000002.672248267.0000000003BFD000.00000004.00000800.00020000.00000000.sdmp, SAaX2wNRn2.exe, 00000001.00000002.660971375.0000000002980000.00000004.00000800.00020000.00000000.sdmp, SAaX2wNRn2.exe, 00000001.00000002.684765718.0000000006B90000.00000004.08000000.00040000.00000000.sdmp, SAaX2wNRn2.exe, 00000001.00000002.672248267.00000000039F8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAaX2wNRn2.exe, 00000001.00000002.660971375.0000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
141.98.6.167	jasonbourneblack.ddns.net	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878777
Start date and time:	2023-05-31 07:51:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 20s
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:	18
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:	SAaX2wNRn2.exe
Original Sample Name:	e89323dd0063fb87b2115af014bbaf94.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@24/11@17/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.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.
- VT rate limit hit for: SAaX2wNRn2.exe

Simulations

Behavior and APIs

Time	Type	Description
07:52:05	API Interceptor	980x Sleep call for process: SAaX2wNRn2.exe modified
07:52:08	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
07:52:10	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\SAaX2wNRn2.exe" s>$(Arg0)
07:52:11	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
07:52:14	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\SAaX2wNRn2.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1107968

Entropy (8bit):	7.681342200669093
Encrypted:	false
SSDEEP:	24576:WkJLaVUH999a0EXC/swhOm5inc8NRLICAWVfjJGXQn+DxkIRZ:BNBH9a0WImm5ic8TJlGAn+Fklb
MD5:	E89323DD0063FB87B2115AF014BBAF94
SHA1:	788E5FCAE9E19827A9E2A3238CF17C50A737D948
SHA-256:	70D856CFC4E27C7CA18C939FD13FB989A308C64C0CD78D5D6F07759CC355C3DB
SHA-512:	BD66EC1C94DA96F51FC4487DA13E77710FF0F1DADE38859BDF3F86F3D42BB8DC4E955D79E29273D3B555C6773D8C98676BD9A0F670345FD9D7EE6782F13867A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6~.....0..... .....@.. .....@..... ..@.....O..... .....p..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H..... I.....0.....r...ps.....~.....+..*".(.....*..0..`.....s....}.....}.....(.....s....s.....o.....{....o.....o..... ....(.....(.....o.....*6.sM...(.....*..*....0.....~.....o ...o!.....r"..p.o"....L...o#....L...o$.....r0..p.o%....L...o#....L...o&.....r<..p.o'....L...o#....L...o(.....rF..p.o)....L...o#....L...o*.....&.. ..*.....0..m.....s+....+M...+3...o,...o-....

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

Process:	C:\Users\user\Desktop\SAaX2wNRn2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SAaX2wNRn2.exe.log

Process:	C:\Users\user\Desktop\SAaX2wNRn2.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\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\Temp\tmp1C83.tmp

Process:	C:\Users\user\Desktop\SAaX2wNRn2.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.103160930415285
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PmlxtnːcbkoL600QydbQxIYODOLedq3SQj
MD5:	0F6280DDBDCD8BA3DD05C3A2B2830CE1
SHA1:	54ADF97784C03D8E5F0E1495B0CB1AC7D682D0CA
SHA-256:	E1F4397A5EBB7CC9AD989E0E5D4A2ABB8F4A58090E902B8E4A4B41AD8C921C1C
SHA-512:	F80AEA64F216E3388DDD969917BC64B322DE1ED54EB8350A825CF0CA7B04DDB78C06B0391AD666D040A2CA4EBC512B67A4753B6FD875AB306E90DBB3E2F7745
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\tmp1E68.tmp

Process:	C:\Users\user\Desktop\SAaX2wNRn2.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/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtnːcbk4oL600QydbQxIYODOLedq3S3j
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\SAaX2wNRn2.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false

SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
Malicious:	false
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\SAaX2wNRn2.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:K:K
MD5:	CED92A1312CEBF2C089EECDAFE3BE2E4
SHA1:	4688DB535ACE3DBE636AF7D01F850E91286E0044
SHA-256:	E81032B5009AEBCC130758D8EFAFDD937ADCAC2900495E78DA0D8F7DB8835790
SHA-512:	5002352CA33AF2559D3631D7B19C9871156812E274AB2DB77C8440747E0350A82686FE29AF4C14BA0BCD51775FA17C9BC8F8D9A4941E7585E8A81B1CA1732076
Malicious:	**true**
Preview:	>{...a.H

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

Process:	C:\Users\user\Desktop\SAaX2wNRn2.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

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

Process:	C:\Users\user\Desktop\SAaX2wNRn2.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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.""..v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...I.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..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\SAaX2wNRn2.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.405822250285692
Encrypted:	false
SSDEEP:	3:oNUWJRW2N1Sr7XJ:oNNJA2N1S3Z
MD5:	C5309FC2F2D48EE1E1D12676BE13EE52
SHA1:	C93663839AE1AA83A8D59A56E83839120C449C97
SHA-256:	792F2B8B322E2CD8ABE3AE852092273883A7F6133A3FB0C0FBFD240EA809A624
SHA-512:	13B00B680C2BBBA2791FAAD9D9BD420DA908BFCF6E331C3EC9C9272CE6AD858053331F6FF9869F8EE1B6244375844A4278F1139C9ED78897CA077B8CE8F7AA8
Malicious:	false
Preview:	C:\Users\user\Desktop\SAaX2wNRn2.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.681342200669093
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SAaX2wNRn2.exe
File size:	1107968
MD5:	e89323dd0063fb87b2115af014bbaf94
SHA1:	788e5fcae9e19827a9e2a3238cf17c50a737d948
SHA256:	70d856cfc4e27c7ca18c939fd13fb989a308c64c0cd78d5d6f07759cc355c3db
SHA512:	bd66ec1c94da96f51fc4487da13e77710ff0f1dade38859bdf3f86f3d42bb8dc4e955d79e29273d3b555c6773d8c98676bd9a0f670345fd9d7ee6782f13867aa
SSDEEP:	24576:WkJLaVUH999a0EXC/swhOm5inc8NRLICAWVfjJGXQn+DxkIRZ:BNBH9a0WImm5ic8TJlGAn+Fklb
TLSH:	1235F14463BB8F2BD47B57F24610623087FA6AA9347EE32A8ED261DF1575F404E01B1B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6~.....0..... .....@.. .....@.....@.....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x50fce6
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:	0xA87E36FB [Thu Jul 31 02:24:59 2059 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 byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10fc94	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x110000	0x5d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x112000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10c0e4	0x70	.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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x10dcec	0x10de00	False	0.8788990128531727	data	7.686102487900815	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x110000	0x5d0	0x600	False	0.4322916666666667	data	4.146225266616758	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x112000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x110090	0x340	data		
RT_MANIFEST	0x1103e0	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

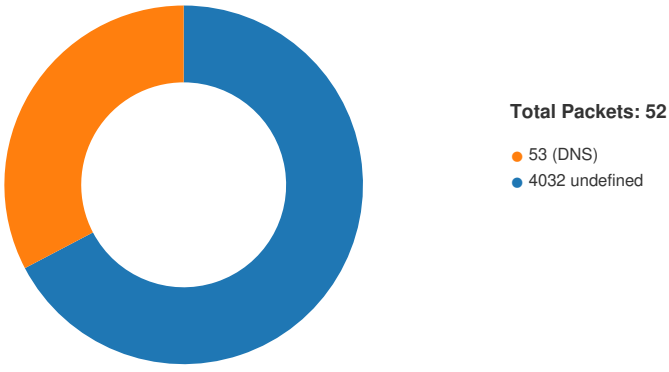
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5141.98.6.1674972340322816766 05/31/23-07:53:03.283583	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674971640322816766 05/31/23-07:52:13.461105	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674971840322025019 05/31/23-07:52:31.617417	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972840322025019 05/31/23-07:53:33.869411	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972940322816766 05/31/23-07:53:43.288922	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49729	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674973340322816766 05/31/23-07:54:08.525317	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49733	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674973240322025019 05/31/23-07:54:01.126019	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674971940322816766 05/31/23-07:52:40.572861	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	4032	192.168.2.5	141.98.6.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5141.98.6.1674971940322025019 05/31/23-07:52:39.496237	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972240322025019 05/31/23-07:52:54.172177	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674973040322816766 05/31/23-07:53:49.430104	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49730	4032	192.168.2.5	141.98.6.167
141.98.6.167192.168.2.54032497182810290 05/31/23-07:52:32.211435	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	4032	49718	141.98.6.167	192.168.2.5
192.168.2.5141.98.6.1674973240322816718 05/31/23-07:54:02.704983	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49732	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674971640322025019 05/31/23-07:52:11.267334	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972040322816766 05/31/23-07:52:48.788255	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972440322816766 05/31/23-07:53:09.525595	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49724	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972540322025019 05/31/23-07:53:15.239239	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674973140322025019 05/31/23-07:53:54.566547	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972940322025019 05/31/23-07:53:42.302533	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674973140322816766 05/31/23-07:53:56.008756	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49731	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674971840322816766 05/31/23-07:52:32.730530	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972840322816766 05/31/23-07:53:36.859358	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49728	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972340322025019 05/31/23-07:53:02.033758	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	4032	192.168.2.5	141.98.6.167
141.98.6.167192.168.2.54032497332841753 05/31/23-07:54:23.318530	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4032	49733	141.98.6.167	192.168.2.5
192.168.2.5141.98.6.1674972040322025019 05/31/23-07:52:47.324081	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674972640322025019 05/31/23-07:53:20.721069	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674973040322025019 05/31/23-07:53:48.374058	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	4032	192.168.2.5	141.98.6.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
141.98.6.167192.168.2.54 032497252841753 05/31/23-07:53:15.269919	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4032	49725	141.98.6.167	192.168.2.5
141.98.6.167192.168.2.54 032497172841753 05/31/23-07:52:25.058340	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4032	49717	141.98.6.167	192.168.2.5
192.168.2.5141.98.6.1674 972240322816766 05/31/23-07:52:55.998811	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 972440322025019 05/31/23-07:53:08.375676	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 972740322816766 05/31/23-07:53:28.901780	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49727	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 971740322816766 05/31/23-07:52:22.187780	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 971740322025019 05/31/23-07:52:20.026839	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 972640322816766 05/31/23-07:53:21.715954	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49726	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 972040322816718 05/31/23-07:52:47.571898	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49720	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 973240322816766 05/31/23-07:54:02.704983	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49732	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 972740322025019 05/31/23-07:53:27.404072	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	4032	192.168.2.5	141.98.6.167
192.168.2.5141.98.6.1674 973340322025019 05/31/23-07:54:08.288405	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	4032	192.168.2.5	141.98.6.167

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 07:52:11.139539957 CEST	49716	4032	192.168.2.5	141.98.6.167

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 07:52:11.166393995 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.166547060 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.267333984 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.344276905 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.344360113 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.378912926 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.397016048 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.425708055 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.473263979 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.494035959 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.577244043 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.680847883 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.680958986 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.680986881 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.681005955 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.681045055 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.681086063 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.708596945 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708760023 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708786964 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708810091 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708836079 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708858013 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708863974 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.708882093 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708906889 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.708911896 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.708911896 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.710009098 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.739830017 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.739860058 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.739896059 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.739939928 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.739964008 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.739985943 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740015984 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740016937 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.740040064 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740063906 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.740067959 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740086079 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.740092993 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740118980 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740143061 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740156889 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.740175962 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740181923 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.740204096 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740227938 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.740242004 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.740253925 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.743238926 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.766690969 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.766854048 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.766884089 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.766913891 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.766921997 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.766946077 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.766971111 CEST	49716	4032	192.168.2.5	141.98.6.167

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 07:52:11.766983986 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767015934 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767040014 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767040968 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767071009 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767076969 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767098904 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767122984 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767146111 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767165899 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767168999 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767193079 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767195940 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767220020 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767244101 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767261982 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767268896 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767285109 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767293930 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767318010 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767339945 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767359972 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767363071 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767384052 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767390013 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767415047 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767436981 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767460108 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767467022 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767482996 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767493963 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767508030 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767530918 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.767551899 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.767571926 CEST	49716	4032	192.168.2.5	141.98.6.167
May 31, 2023 07:52:11.769560099 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.769594908 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.769618034 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.769642115 CEST	4032	49716	141.98.6.167	192.168.2.5
May 31, 2023 07:52:11.769712925 CEST	49716	4032	192.168.2.5	141.98.6.167

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 07:52:11.096995115 CEST	51484	53	192.168.2.5	8.8.8.8
May 31, 2023 07:52:11.132067919 CEST	53	51484	8.8.8.8	192.168.2.5
May 31, 2023 07:52:19.967236996 CEST	63446	53	192.168.2.5	8.8.8.8
May 31, 2023 07:52:19.994401932 CEST	53	63446	8.8.8.8	192.168.2.5
May 31, 2023 07:52:31.550893068 CEST	56751	53	192.168.2.5	8.8.8.8
May 31, 2023 07:52:31.574661016 CEST	53	56751	8.8.8.8	192.168.2.5
May 31, 2023 07:52:39.431263924 CEST	55039	53	192.168.2.5	8.8.8.8
May 31, 2023 07:52:39.459728003 CEST	53	55039	8.8.8.8	192.168.2.5
May 31, 2023 07:52:47.050631046 CEST	60975	53	192.168.2.5	8.8.8.8
May 31, 2023 07:52:47.079140902 CEST	53	60975	8.8.8.8	192.168.2.5
May 31, 2023 07:52:54.107012987 CEST	55068	53	192.168.2.5	8.8.8.8
May 31, 2023 07:52:54.142549038 CEST	53	55068	8.8.8.8	192.168.2.5
May 31, 2023 07:53:01.813743114 CEST	56682	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:01.833653927 CEST	53	56682	8.8.8.8	192.168.2.5
May 31, 2023 07:53:08.316106081 CEST	58532	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 07:53:08.344156027 CEST	53	58532	8.8.8.8	192.168.2.5
May 31, 2023 07:53:15.173487902 CEST	62659	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:15.208040953 CEST	53	62659	8.8.8.8	192.168.2.5
May 31, 2023 07:53:20.671876907 CEST	58581	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:20.692138910 CEST	53	58581	8.8.8.8	192.168.2.5
May 31, 2023 07:53:27.353101015 CEST	56263	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:27.373688936 CEST	53	56263	8.8.8.8	192.168.2.5
May 31, 2023 07:53:33.785145044 CEST	65513	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:33.819334030 CEST	53	65513	8.8.8.8	192.168.2.5
May 31, 2023 07:53:42.233668089 CEST	56687	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:42.262104034 CEST	53	56687	8.8.8.8	192.168.2.5
May 31, 2023 07:53:48.309499025 CEST	64419	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:48.344185114 CEST	53	64419	8.8.8.8	192.168.2.5
May 31, 2023 07:53:54.513269901 CEST	52688	53	192.168.2.5	8.8.8.8
May 31, 2023 07:53:54.533252001 CEST	53	52688	8.8.8.8	192.168.2.5
May 31, 2023 07:54:01.059043884 CEST	61344	53	192.168.2.5	8.8.8.8
May 31, 2023 07:54:01.094084024 CEST	53	61344	8.8.8.8	192.168.2.5
May 31, 2023 07:54:08.144618988 CEST	53972	53	192.168.2.5	8.8.8.8
May 31, 2023 07:54:08.171468973 CEST	53	53972	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 07:52:11.096995115 CEST	192.168.2.5	8.8.8.8	0xd0ef	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:19.967236996 CEST	192.168.2.5	8.8.8.8	0xe4aa	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:31.550893068 CEST	192.168.2.5	8.8.8.8	0x54aa	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:39.431263924 CEST	192.168.2.5	8.8.8.8	0xebf7	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:47.050631046 CEST	192.168.2.5	8.8.8.8	0x42de	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:54.107012987 CEST	192.168.2.5	8.8.8.8	0x66fe	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:01.813743114 CEST	192.168.2.5	8.8.8.8	0x5d11	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:08.316106081 CEST	192.168.2.5	8.8.8.8	0x3c6b	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:15.173487902 CEST	192.168.2.5	8.8.8.8	0x1b8a	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:20.671876907 CEST	192.168.2.5	8.8.8.8	0xf72c	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:27.353101015 CEST	192.168.2.5	8.8.8.8	0x7449	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:33.785145044 CEST	192.168.2.5	8.8.8.8	0x351e	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:42.233668089 CEST	192.168.2.5	8.8.8.8	0xd34	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:48.309499025 CEST	192.168.2.5	8.8.8.8	0xd633	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:54.513269901 CEST	192.168.2.5	8.8.8.8	0xdf79	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:54:01.059043884 CEST	192.168.2.5	8.8.8.8	0x8bef	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 07:54:08.144618988 CEST	192.168.2.5	8.8.8.8	0x537b	Standard query (0)	jasonbourneblack.ddns.net	A (IP address)	IN (0x0001)	false

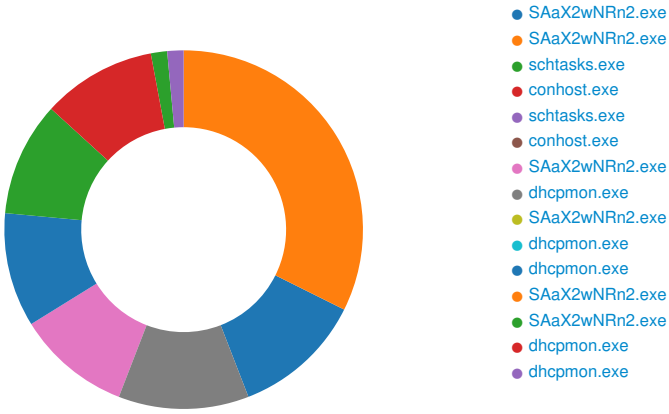
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 07:52:11.132067919 CEST	8.8.8.8	192.168.2.5	0xd0ef	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 07:52:19.994401932 CEST	8.8.8.8	192.168.2.5	0xe4aa	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:31.574661016 CEST	8.8.8.8	192.168.2.5	0x54aa	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:39.459728003 CEST	8.8.8.8	192.168.2.5	0xebf7	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:47.079140902 CEST	8.8.8.8	192.168.2.5	0x42de	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:52:54.142549038 CEST	8.8.8.8	192.168.2.5	0x66fe	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:01.833653927 CEST	8.8.8.8	192.168.2.5	0x5d11	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:08.344156027 CEST	8.8.8.8	192.168.2.5	0x3c6b	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:15.208040953 CEST	8.8.8.8	192.168.2.5	0x1b8a	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:20.692138910 CEST	8.8.8.8	192.168.2.5	0xf72c	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:27.373688936 CEST	8.8.8.8	192.168.2.5	0x7449	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:33.819334030 CEST	8.8.8.8	192.168.2.5	0x351e	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:42.262104034 CEST	8.8.8.8	192.168.2.5	0xd34	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:48.344185114 CEST	8.8.8.8	192.168.2.5	0xd633	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:53:54.533252001 CEST	8.8.8.8	192.168.2.5	0xdf79	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:54:01.094084024 CEST	8.8.8.8	192.168.2.5	0x8bef	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false
May 31, 2023 07:54:08.171468973 CEST	8.8.8.8	192.168.2.5	0x537b	No error (0)	jasonbourneblack.ddns.net		141.98.6.167	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SAaX2wNRn2.exe PID: **2152**, Parent PID: **3324**

General

Target ID:	0
Start time:	07:52:03
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Imagebase:	0x310000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
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: 00000000.00000002.396639113.0000000003771000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.396639113.0000000003771000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.396639113.0000000003771000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.396639113.0000000003771000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.396639113.000000000438A000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.396639113.000000000438A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.396639113.000000000438A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.396639113.000000000438A000.00000004.00000800.00020000.00000000.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	7222CF06	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	7222CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SAaX2wNRn2.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SAaX2wNRn2.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	7253C907	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: SAaX2wNRn2.exe PID: **2888**, Parent PID: **2152**

General

Target ID:	1
Start time:	07:52:06
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Imagebase:	0x470000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
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: 00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.684510708.0000000006B60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000001.00000002.672248267.0000000003BFD000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.672248267.0000000003BFD000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.684765718.0000000006B90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.684765718.0000000006B90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.684765718.0000000006B90000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.684765718.0000000006B90000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.681445042.0000000004FA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.681445042.0000000004FA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.681445042.0000000004FA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.681445042.0000000004FA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.684858574.0000000006BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.684858574.0000000006BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.684858574.0000000006BA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.684858574.0000000006BA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000001.00000002.660971375.0000000002980000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.660971375.0000000002980000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.684333491.0000000006A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.684333491.0000000006A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.684333491.0000000006A10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.684333491.0000000006A10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.683574588.0000000006360000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.683574588.0000000006360000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.683574588.0000000006360000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.683574588.0000000006360000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.672248267.0000000003901000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.684621973.0000000006B70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.684621973.0000000006B70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.684621973.0000000006B70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.684621973.0000000006B70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.685185862.0000000006BD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.685185862.0000000006BD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.685185862.0000000006BD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.685185862.0000000006BD0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.683481713.0000000006350000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.683481713.0000000006350000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.683481713.0000000006350000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.683481713.0000000006350000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.684687442.0000000006B80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.684687442.0000000006B80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.684687442.0000000006B80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.684687442.0000000006B80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.660971375.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.660971375.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.660971375.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.681733074.00000000051B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.681733074.00000000051B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.681733074.00000000051B0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.681733074.00000000051B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.681733074.00000000051B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.684948679.0000000006BB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.684948679.0000000006BB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.684948679.0000000006BB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.684948679.0000000006BB0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.685278523.0000000006BE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.685278523.0000000006BE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.685278523.0000000006BE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.685278523.0000000006BE0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.685898407.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.685898407.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.685898407.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.685898407.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000003.404728224.0000000000B2A000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.672248267.00000000039F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.672248267.00000000039F8000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.672248267.00000000039F8000.00000004.00000800.00020000.00000000.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	7222CF06	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	7222CF06	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	7107BEFF	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	71071E60	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	7107BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7107DD66	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	7107DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1C83.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	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	71071E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1E68.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	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	7107BEFF	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	7107BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	14	71071E60	CreateFileW
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	71071E60	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	71071E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1C83.tmp	success or wait	1	71076A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1E68.tmp	success or wait	1	71076A95	DeleteFileW
C:\Users\user\Desktop\SAaX2wNRn2.exe:Zone.Identifier	success or wait	1	70FF2935	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	3e 7b fd fd fd 61 fd 48	>{aH	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 36 7e fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 10 00 00 08 00 00 00 00 00 00 fd fd 10 00 00 20 00 00 00 00 11 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 11 00 00 02 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.$PEL6~0 @ @@	success or wait	5	7107DD66	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	7107DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1C83.tmp	0	1301	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	71071B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	38	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 53 41 61 58 32 77 4e 52 6e 32 2e 65 78 65	C:\Users\user\Desktop\SAaX2wNRn2.exe	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1E68.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	71071B4F	WriteFile
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	17	71071B4F	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	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	71071B4F	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	721ED72F	unknown
C:\Users\user\Desktop\SAaX2wNRn2.exe	unknown	4096	success or wait	1	721ED72F	unknown
C:\Users\user\Desktop\SAaX2wNRn2.exe	unknown	512	success or wait	1	721ED72F	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	7107646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **5312**, Parent PID: **2888**

General

Target ID:	2
Start time:	07:52:08
Start date:	31/05/2023
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\tmp1C83.tmp
Imagebase:	0x1190000
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\tmp1C83.tmp	unknown	2	success or wait	1	119AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1C83.tmp	unknown	1302	success or wait	1	119ABD9	ReadFile

Analysis Process: conhost.exe PID: **4048**, Parent PID: **5312**

General

Target ID:	3
Start time:	07:52:08
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5744**, Parent PID: **2888**

General

Target ID:	4
Start time:	07:52:09
Start date:	31/05/2023
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\tmp1E68.tmp
Imagebase:	0x1190000
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\tmp1E68.tmp	unknown	2	success or wait	1	119AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1E68.tmp	unknown	1311	success or wait	1	119ABD9	ReadFile

Analysis Process: conhost.exe PID: **760**, Parent PID: **5744**

General

Target ID:	5
Start time:	07:52:09
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SAaX2wNRn2.exe PID: **2244**, Parent PID: **1084**

General

Target ID:	6
Start time:	07:52:11
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SAaX2wNRn2.exe 0
Imagebase:	0xb50000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
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	7222CF06	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	7222CF06	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **2844**, Parent PID: **1084**

General

Target ID:	7
Start time:	07:52:11
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x750000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, 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	7222CF06	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	7222CF06	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	7253C78D	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	7253C907	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: SAaX2wNRn2.exe PID: **6852**, Parent PID: **2244**

General

Target ID:	10
Start time:	07:52:16
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Imagebase:	0xd0000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **6744**, Parent PID: **2844**

General

Target ID:	11
Start time:	07:52:16
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x340000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **5788**, Parent PID: **2844**

General

Target ID:	12
Start time:	07:52:16
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xec0000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.463275758.00000000042F6000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.463275758.0000000004289000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.458436332.0000000003281000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.458436332.0000000003281000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.458436332.0000000003281000.00000004.00000800.00020000.00000000.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	7222CF06	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	7222CF06	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: SAaX2wNRn2.exe PID: **5708**, Parent PID: **2244**

General

Target ID:	13
Start time:	07:52:16

Start date:	31/05/2023
Path:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Imagebase:	0xc0000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SAaX2wNRn2.exe PID: **6840**, Parent PID: **2244**

General

Target ID:	14
Start time:	07:52:17
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SAaX2wNRn2.exe
Imagebase:	0xbe0000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
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: 0000000E.00000002.450850684.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.450850684.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.450850684.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.450850684.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.462495853.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.462495853.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.462495853.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

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	7222CF06	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	7222CF06	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	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	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **4984**, Parent PID: **3324**

General

Target ID:	15
Start time:	07:52:17
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x2c0000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

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	7222CF06	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	7222CF06	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **3712**, Parent PID: **4984**

General

Target ID:	16
Start time:	07:52:31
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xe30000
File size:	1107968 bytes
MD5 hash:	E89323DD0063FB87B2115AF014BBAF94
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly