ID: 876048
Sample Name: jw2ILbVCX7.exe
Cookbook: default.jbs
Time: 09:29:22
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report jw2ILbVCX7.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 5
Threatname: NanoCore 5
Yara Signatures 5
Initial Sample 5
Dropped Files 6
Memory Dumps 7
Unpacked PEs 7
Sigma Signatures 8
AV Detection 8
E-Banking Fraud 8
Persistence and Installation Behavior 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Snort Signatures 8
Joe Sandbox Signatures 10
AV Detection 10
Networking 10
E-Banking Fraud 10
Operating System Destruction 10
System Summary 11
Data Obfuscation 11
Boot Survival 11
Hooking and other Techniques for Hiding and Protection 11
Stealing of Sensitive Information 11
Remote Access Functionality 11
Mitre Att&ck Matrix 11
Behavior Graph 12
Screenshots 12
Thumbnails 12
Antivirus, Machine Learning and Genetic Malware Detection 13
Initial Sample 13
Dropped Files 13
Unpacked PE Files 14
Domains 14
URLs 14
Domains and IPs 14
Contacted Domains 14
Contacted URLs 14
World Map of Contacted IPs 14
Public IPs 15
General Information 15
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 16
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier 17
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log 17
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\jw2ILbVCX7.exe.log 17
C:\Users\user\AppData\Local\Temp\tmpDC9A.tmp 18
C:\Users\user\AppData\Local\Temp\tmpDDF3.tmp 18
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 18
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat 19
Static File Info 19
General 19

File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Data Directories 21
Sections 22
Resources 22
Imports 22
Network Behavior 22
Snort IDS Alerts 22
Network Port Distribution 23
TCP Packets 23
UDP Packets 25
DNS Queries 26
DNS Answers 26
Statistics 27
Behavior 27
System Behavior 28
Analysis Process: jw2lLbVCX7.exePID: 6980, Parent PID: 3452 28
General 28
File Activities 29
File Created 29
File Deleted 30
File Written 30
File Read 31
Registry Activities 32
Key Value Created 32
Analysis Process: schtasks.exePID: 7004, Parent PID: 6980 32
General 32
File Activities 32
File Read 32
Analysis Process: conhost.exePID: 7068, Parent PID: 7004 32
General 32
Analysis Process: schtasks.exePID: 1004, Parent PID: 6980 33
General 33
File Activities 33
File Read 33
Analysis Process: conhost.exePID: 2576, Parent PID: 1004 33
General 33
Analysis Process: jw2lLbVCX7.exePID: 6112, Parent PID: 1080 33
General 33
File Activities 34
File Created 34
File Written 34
File Read 34
Analysis Process: dhcpmon.exePID: 5748, Parent PID: 1080 35
General 35
File Activities 35
File Created 35
File Written 35
File Read 36
Analysis Process: dhcpmon.exePID: 7076, Parent PID: 3452 36
General 36
File Activities 36
File Created 36
File Read 37
Disassembly 37

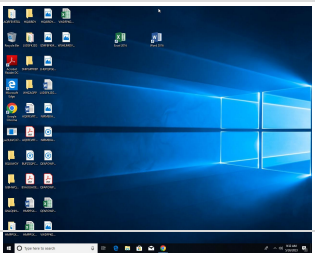
Windows Analysis Report

jw2ILbVCX7.exe

Overview

General Information

Sample Name:	jw2ILbVCX7.exe
Original Sample Name:	beca1cb2ead4…
Analysis ID:	876048
MD5:	beca1cb2ead4…
SHA1:	3251edb9b99c…
SHA256:	ee6820bbca27…
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

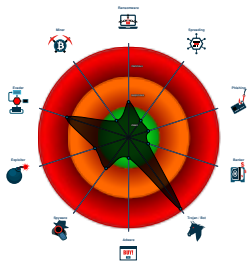
Nanocore

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
- Antivirus / Scanner detection for sub…
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT

Classification



Process Tree

- **System is w10x64**
- jw2ILbVCX7.exe (PID: 6980 cmdline: C:\Users\user\Desktop\jw2ILbVCX7.exe MD5: BECA1CB2EAD4D465A208217AC1B189D1)
  - schtasks.exe (PID: 7004 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpDC9A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1004 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpDDF3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- jw2ILbVCX7.exe (PID: 6112 cmdline: C:\Users\user\Desktop\jw2ILbVCX7.exe 0 MD5: BECA1CB2EAD4D465A208217AC1B189D1)
- dhcpmon.exe (PID: 5748 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: BECA1CB2EAD4D465A208217AC1B189D1)
- dhcpmon.exe (PID: 7076 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: BECA1CB2EAD4D465A208217AC1B189D1)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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/bay world-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": "8a269adf-55ef-40ff-8dd6-457050ba",
  "Group": "dec2nd",
  "Domain1": "december2n.duckdns.org",
  "Domain2": "december2nd.ddns.net",
  "Port": 60451,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
jw2ILbVCX7.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
jw2ILbVCX7.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
jw2ILbVCX7.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
jw2ILbVCX7.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	0xfef5:$x1: NanoCore Client 0xff05:$x1: NanoCore Client 0x1014d:$x2: NanoCore.ClientPlugin 0x1018d:$x3: NanoCore.ClientPluginHost 0x10142:$i1: IClientApp 0x10163:$i2: IClientData 0x1016f:$i3: IClientNetwork 0x1017e:$i4: IClientAppHost 0x101a7:$i5: IClientDataHost 0x101b7:$i6: IClientLoggingHost 0x101ca:$i7: IClientNetworkHost 0x101dd:$i8: IClientUIHost 0x101eb:$i9: IClientNameObjectCollection 0x10207:$i10: IClientReadOnlyNameObjectCollection 0xff54:$s1: ClientPlugin 0x10156:$s1: ClientPlugin 0x1064a:$s2: EndPoint 0x10653:$s3: IPAddress 0x1065d:$s4: IPEndPoint 0x12093:$s6: get_ClientSettings 0x12637:$s7: get_Connected
jw2ILbVCX7.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfef5:$a: NanoCore 0xff05:$a: NanoCore 0x10139:$a: NanoCore 0x1014d:$a: NanoCore 0x1018d:$a: NanoCore 0xff54:$b: ClientPlugin 0x10156:$b: ClientPlugin 0x10196:$b: ClientPlugin 0x1007b:$c: ProjectData 0x10a82:$d: DESCrypto 0x1844e:$e: KeepAlive 0x1643c:$g: LogClientMessage 0x12637:$i: get_Connected 0x10db8:$j: #=q 0x10de8:$j: #=q 0x10e04:$j: #=q 0x10e34:$j: #=q 0x10e50:$j: #=q 0x10e6c:$j: #=q 0x10e9c:$j: #=q 0x10eb8:$j: #=q
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0x1018d:$x1: NanoCore.ClientPluginHost 0x101ca:$x2: IClientNetworkHost 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0xff05:$x1: NanoCore Client.exe 0x1018d:$x2: NanoCore.ClientPluginHost 0x117c6:$s1: PluginCommand 0x117ba:$s2: FileCommand 0x1266b:$s3: PipeExists 0x18422:$s4: PipeCreated 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	0xfef5:$x1: NanoCore Client 0xff05:$x1: NanoCore Client 0x1014d:$x2: NanoCore.ClientPlugin 0x1018d:$x3: NanoCore.ClientPluginHost 0x10142:$i1: IClientApp 0x10163:$i2: IClientData 0x1016f:$i3: IClientNetwork 0x1017e:$i4: IClientAppHost 0x101a7:$i5: IClientDataHost 0x101b7:$i6: IClientLoggingHost 0x101ca:$i7: IClientNetworkHost 0x101dd:$i8: IClientUIHost 0x101eb:$i9: IClientNameObjectCollection 0x10207:$i10: IClientReadOnlyNameObjectCollection 0xff54:$s1: ClientPlugin 0x10156:$s1: ClientPlugin 0x1064a:$s2: EndPoint 0x10653:$s3: IPAddress 0x1065d:$s4: IPEndPoint 0x12093:$s6: get_ClientSettings 0x12637:$s7: get_Connected

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfef5:$a: NanoCore 0xff05:$a: NanoCore 0x10139:$a: NanoCore 0x1014d:$a: NanoCore 0x1018d:$a: NanoCore 0xff54:$b: ClientPlugin 0x10156:$b: ClientPlugin 0x10196:$b: ClientPlugin 0x1007b:$c: ProjectData 0x10a82:$d: DESCrypto 0x1844e:$e: KeepAlive 0x1643c:$g: LogClientMessage 0x12637:$i: get_Connected 0x10db8:$j: #=q 0x10de8:$j: #=q 0x10e04:$j: #=q 0x10e34:$j: #=q 0x10e50:$j: #=q 0x10e6c:$j: #=q 0x10e9c:$j: #=q 0x10eb8:$j: #=q
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.388017452.0000000002831000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000006.00000002.388017452.0000000002831000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0x23ba3:$a: NanoCore 0x23bfc:$a: NanoCore 0x23c39:$a: NanoCore 0x23cb2:$a: NanoCore 0x29496:$a: NanoCore 0x294e0:$a: NanoCore 0x296ca:$a: NanoCore 0x23c05:$b: ClientPlugin 0x23c42:$b: ClientPlugin 0x24540:$b: ClientPlugin 0x2454d:$b: ClientPlugin 0x2922f:$b: ClientPlugin 0x2949f:$b: ClientPlugin 0x294e9:$b: ClientPlugin 0x29a01:$c: ProjectData 0x19361:$e: KeepAlive 0x2408d:$g: LogClientMessage 0x298f4:$g: LogClientMessage 0x2400d:$i: get_Connected 0x193fb:$j: #=q 0x1942b:$j: #=q
00000006.00000002.388017452.0000000002831000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0x23c39:$a1: NanoCore.ClientPluginHost 0x29496:$a1: NanoCore.ClientPluginHost 0x23bfc:$a2: NanoCore.ClientPlugin 0x294e0:$a2: NanoCore.ClientPlugin 0x1cb4c:$b1: get_BuilderSettings 0x23fd0:$b1: get_BuilderSettings 0x23c87:$b4: IClientAppHost 0x24041:$b6: AddHostEntry 0x1cabb:$b7: LogClientException 0x240b0:$b7: LogClientException 0x24025:$b8: PipeExists 0x23c74:$b9: IClientLoggingHost 0x294b0:$b9: IClientLoggingHost
00000000.00000002.645832197.0000000005930000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0x1646:$x1: NanoCore.ClientPluginHost
00000000.00000002.645832197.0000000005930000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0x1646:$x2: NanoCore.ClientPluginHost 0x1724:$s4: PipeCreated 0x1660:$s5: IClientLoggingHost
Click to see the 32 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.jw2lLbVCX7.exe.5944629.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0xb184:$x1: NanoCore.ClientPluginHost 0xb1b1:$x2: IClientNetworkHost
0.2.jw2lLbVCX7.exe.5944629.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0xb184:$x2: NanoCore.ClientPluginHost 0xc25f:$s4: PipeCreated 0xb19e:$s5: IClientLoggingHost
0.2.jw2lLbVCX7.exe.5944629.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.jw2ILbVCX7.exe.5944629.6.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xb14f:$x2: NanoCore.ClientPlugin • 0xb184:$x3: NanoCore.ClientPluginHost • 0xb143:$i2: IClientData • 0xb165:$i3: IClientNetwork • 0xb174:$i5: IClientDataHost • 0xb19e:$i6: IClientLoggingHost • 0xb1b1:$i7: IClientNetworkHost • 0xb1c4:$i8: IClientUIHost • 0xb1d2:$i9: IClientNameObjectCollection • 0xb1ee:$i10: IClientReadOnlyNameObjectCollection • 0xaf41:$s1: ClientPlugin • 0xb158:$s1: ClientPlugin • 0x10179:$s6: get_ClientSettings
0.2.jw2ILbVCX7.exe.5944629.6.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xb184:$a1: NanoCore.ClientPluginHost • 0xb14f:$a2: NanoCore.ClientPlugin • 0x100ca:$b1: get_BuilderSettings • 0x10039:$b7: LogClientException • 0xb19e:$b9: IClientLoggingHost
Click to see the 86 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26

Timestamp:	192.168.2.3192.169.69.26496996045120250 19 05/26/23-09:30:25.340331
SID:	2025019
Source Port:	49699
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26

Timestamp:	192.168.2.3192.169.69.26497066045120250 19 05/26/23-09:31:04.760372
SID:	2025019
Source Port:	49706
Destination Port:	60451
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497136045120250195/26/23-09:31:45.263536
SID:	2025019
Source Port:	49713
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497176045120250195/26/23-09:32:11.307312
SID:	2025019
Source Port:	49717
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497076045120250195/26/23-09:31:09.762081
SID:	2025019
Source Port:	49707
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497186045120250195/26/23-09:32:18.263288
SID:	2025019
Source Port:	49718
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497006045120250195/26/23-09:30:30.811034
SID:	2025019
Source Port:	49700
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497126045120250195/26/23-09:31:39.755174
SID:	2025019
Source Port:	49712
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497016045120250195/26/23-09:30:35.827016
SID:	2025019
Source Port:	49701
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.26497056045120250195/26/23-09:30:59.250023

SID:	2025019
Source Port:	49705
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	−
Timestamp:	192.168.2.3192.169.69.26497116045120250 19 05/26/23-09:31:34.268145
SID:	2025019
Source Port:	49711
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	−
Timestamp:	192.168.2.3192.169.69.26497196045120250 19 05/26/23-09:32:23.314247
SID:	2025019
Source Port:	49719
Destination Port:	60451
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration
Multi AV Scanner detection for submitted file
Antivirus / Scanner detection for submitted sample
Antivirus detection for URL or domain
Multi AV Scanner detection for domain / URL
Antivirus detection for dropped file
Multi AV Scanner detection for dropped file
Yara detected Nanocore RAT
Machine Learning detection for sample
Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic
Connects to many ports of the same IP (likely port scanning)
C2 URLs / IPs found in malware configuration
Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

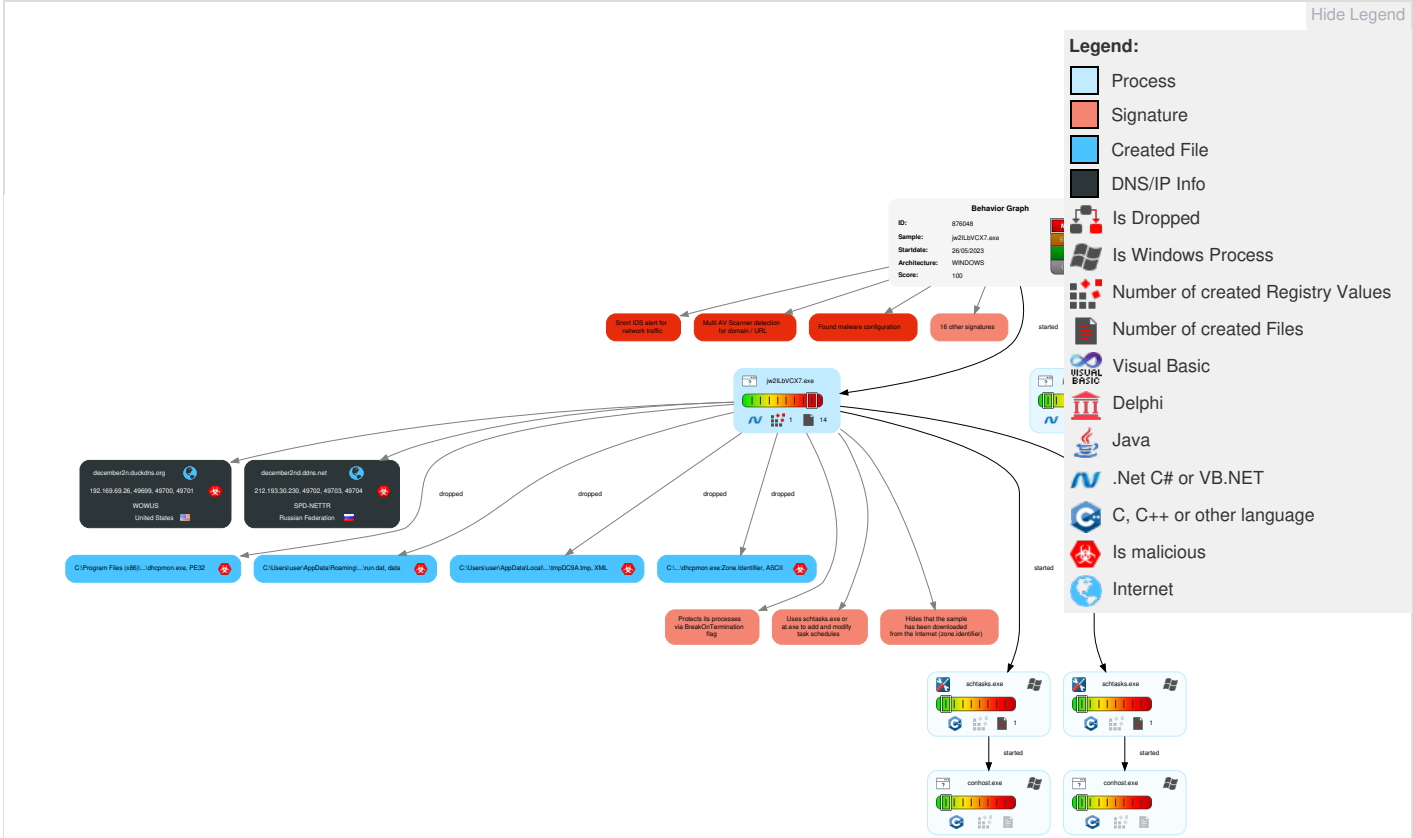
Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

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	2 Obfuscated Files or Information	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 1 Software Packing	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
jw2ILbVCX7.exe	86%	Virustotal		Browse
jw2ILbVCX7.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
jw2ILbVCX7.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
jw2ILbVCX7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
december2nd.ddns.net	17%	Virustotal		Browse
december2n.duckdns.org	19%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
december2nd.ddns.net	17%	Virustotal		Browse
december2n.duckdns.org	100%	Avira URL Cloud	malware	
december2nd.ddns.net	100%	Avira URL Cloud	malware	
december2n.duckdns.org	19%	Virustotal		Browse

Domains and IPs

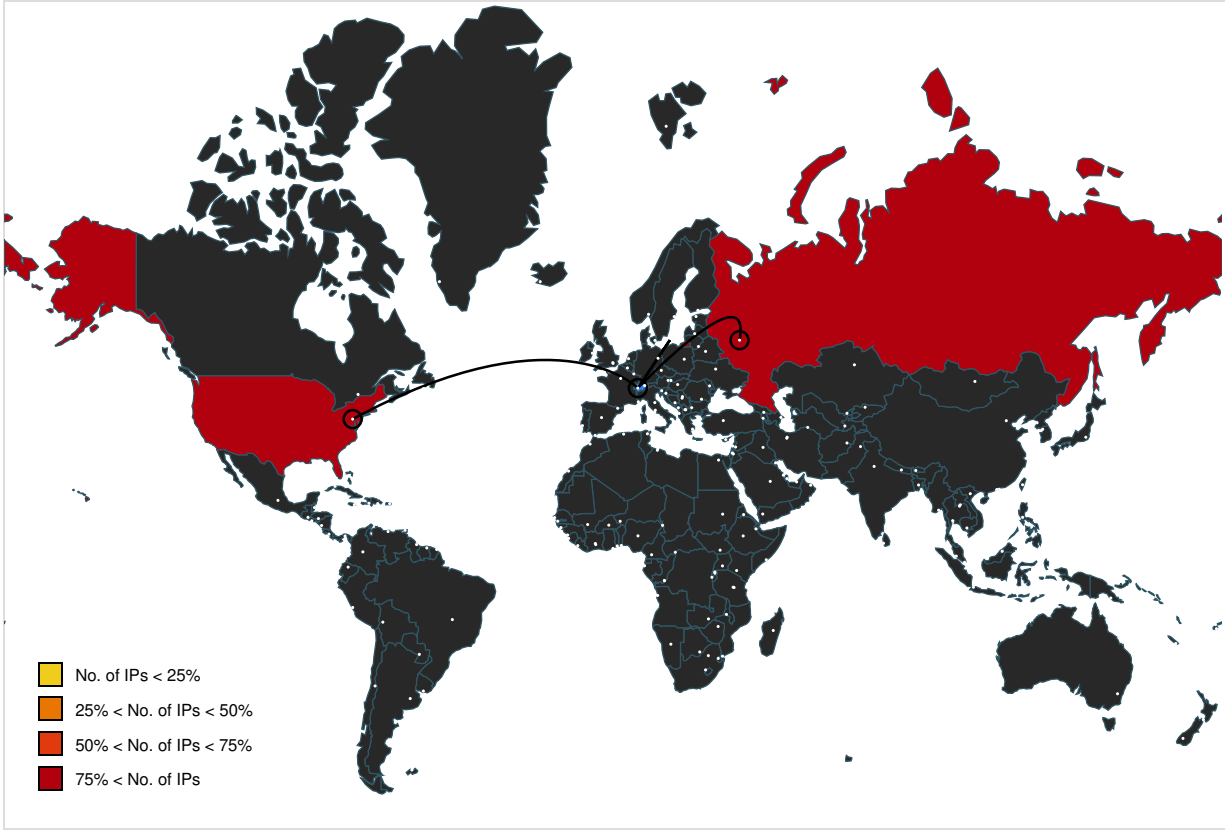
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	212.193.30.230	true	true	• 17%, Virustotal, Browse	unknown
december2n.duckdns.org	192.169.69.26	true	true	• 19%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
december2n.duckdns.org	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.30.230	december2nd.ddns.net	Russian Federation		57844	SPD-NETTR	true
192.169.69.26	december2n.duckdns.org	United States		23033	WOWUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876048
Start date and time:	2023-05-26 09:29:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 14s
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:	12
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:	jw2ILbVCX7.exe
Original Sample Name:	beca1cb2ead4d465a208217ac1b189d1.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/8@22/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:30:23	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\jw2ILbVCX7.exe" s>$(Arg0)
09:30:23	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
09:30:23	API Interceptor	891x Sleep call for process: jw2ILbVCX7.exe modified
09:30:23	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\jw2ILbVCX7.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	215040
Entropy (8bit):	7.469302931020199
Encrypted:	false
SSDEEP:	6144:QLV6Bta6dtJmakIM5v+onU9nYdeCUkuI:QLV6Btpmk8+ononY0CUX
MD5:	BECA1CB2EAD4D465A208217AC1B189D1

SHA1:	3251EDB9B99C9FF7AD8915073C290B4EE68AE6BA
SHA-256:	EE6820BBCA27CF252B5D81CBBF0FE67A85246B4EEA3C584607640D0F8ADDE5E2
SHA-512:	59D1151DF38C4453F9D42622A7B040AAC54FE29F97BFC54EBB551444FACC47A6B31D66A4E7F0BA22A9FF140658E7A27ADD44C33F9A557076CB0AF13D232E8C E
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....~..... .....P.. ....8...W.... ..xz..... ....H.....text..... ....`.reloc.....@..B.rsrc...xz... ...|.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

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

Process:	C:\Users\user\Desktop\jw2ILbVCX7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\jw2ILbVCX7.exe.log

Process:	C:\Users\user\Desktop\jw2ILbVCX7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316

Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpDC9A.tmp

Process:	C:\Users\user\Desktop\jw2ILbVCX7.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.126124822814046
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Gxtn:cbk4oL600QydbQxIYODOLedq3xj
MD5:	A45475C551DF24D890864E53200710D0
SHA1:	3EC83C93F3A5BB082D82488054E41BE48FA58522
SHA-256:	DA1149045379643C10723D4F225CDC0193CA514C0FD314D9B4DE0B29105BF958
SHA-512:	AFF779053DF54FC8F5F5BDD43EE849648EC3A1FC2C5D84186735A5009B21509FB607FD8C6FBC7B1960C8CD7BFE2D6767DE4890DD455774245007C4BAB4702D E
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>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpDDF3.tmp

Process:	C:\Users\user\Desktop\jw2ILbVCX7.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 4
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>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\jw2ILbVCX7.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PjGn:qn

MD5:	C1DB5CC9E0E33ED88D61715E1FBD34F5
SHA1:	9CCB11098559FE79C72D78408FE14549FA4C274F
SHA-256:	C00776E6E49AFD4E941713E88F0002C8631EFB919654600DF0246A573C0A9758
SHA-512:	CC783512BC708CFE1B130ABAF8A7053ECB3DB8AEAC1A92F84460859572A1BD7F9D9906A9E90CCCAF4C20C0FAEE70CB153491908CB481A3F6F9B2F18C997F0 CC
Malicious:	**true**
Preview:	.$...^.H

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

Process:	C:\Users\user\Desktop\jw2ILbVCX7.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.540402352056966
Encrypted:	false
SSDEEP:	3:oNWXp5vPKSJn:oNWXpFRJn
MD5:	35853B6714A1A1C49A5FCF332832D0BC
SHA1:	9DFDFBC08D8F73F905CF11D080E5C4091EA803A1
SHA-256:	0A4BA7D085C2C8DED50425417A0115B13067B2CA7297544981807000D8376CB3
SHA-512:	2259D9DA56EBB4E15BB8EF1592E6AB10AE5E01C59E7E5A3A244ACA48D0CC5F8F8ED4E51851AD023DCFCC4E95BF62707D2D56FFA29F843C55D01636CE8399B 24C
Malicious:	false
Preview:	C:\Users\user\Desktop\jw2ILbVCX7.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.469302931020199
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:	jw2ILbVCX7.exe
File size:	215040
MD5:	beca1cb2ead4d465a208217ac1b189d1
SHA1:	3251edb9b99c9ff7ad8915073c290b4ee68ae6ba
SHA256:	ee6820bbca27cf252b5d81cbbf0fe67a85246b4eea3c584607640d0f8adde5e2
SHA512:	59d1151df38c4453f9d42622a7b040aac54fe29f97bfc54ebb551444facc47a6b31d66a4e7f0ba22a9ff140658e7a27add44c33f9a557076cb0af13d232e8c6e
SSDEEP:	6144:QLV6Bta6dtJmakIM5v+onU9nYdeCUkuI:QLV6Btpmk8+ononY0CUX
TLSH:	3D24CF26BBB8492FE2DF86B9601211529378C2E399C3F3DE18D855B35F6A7E106071D3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....~..... .....P.. .....

File Icon

Icon Hash:	90cececece8e8eb0

Static PE Info

General

Entrypoint:	0x51e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x500000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 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 [00502000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x17a78	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.5945038377192983	data	6.5980598597415945	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x17a78	0x17c00	False	0.9967002467105263	data	7.994814486129098	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x17a20	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3192.169.69.26 49699604512025019 05/26/23-09:30:25.340331	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 49706604512025019 05/26/23-09:31:04.760372	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 49713604512025019 05/26/23-09:31:45.263536	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 49717604512025019 05/26/23-09:32:11.307312	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 49707604512025019 05/26/23-09:31:09.762081	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	60451	192.168.2.3	192.169.69.26

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3192.169.69.26 4971860451202501905/26/23-09:32:18.263288	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970060451202501905/26/23-09:30:30.811034	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971260451202501905/26/23-09:31:39.755174	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970160451202501905/26/23-09:30:35.827016	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970560451202501905/26/23-09:30:59.250023	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971160451202501905/26/23-09:31:34.268145	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	60451	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971960451202501905/26/23-09:32:23.314247	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	60451	192.168.2.3	192.169.69.26

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 60451 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 09:30:24.652987003 CEST	49699	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:25.244465113 CEST	60451	49699	192.169.69.26	192.168.2.3
May 26, 2023 09:30:25.244636059 CEST	49699	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:25.340331078 CEST	49699	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:25.764339924 CEST	60451	49699	192.169.69.26	192.168.2.3
May 26, 2023 09:30:30.446964979 CEST	49700	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:30.760632038 CEST	60451	49700	192.169.69.26	192.168.2.3
May 26, 2023 09:30:30.760843992 CEST	49700	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:30.811033964 CEST	49700	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:31.261578083 CEST	60451	49700	192.169.69.26	192.168.2.3
May 26, 2023 09:30:35.408437014 CEST	49701	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:35.763679028 CEST	60451	49701	192.169.69.26	192.168.2.3
May 26, 2023 09:30:35.763897896 CEST	49701	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:35.827016115 CEST	49701	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:36.258495092 CEST	60451	49701	192.169.69.26	192.168.2.3
May 26, 2023 09:30:40.381091118 CEST	49702	60451	192.168.2.3	212.193.30.230

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 09:30:40.585769892 CEST	60451	49702	212.193.30.230	192.168.2.3
May 26, 2023 09:30:41.287950039 CEST	49702	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:41.493647099 CEST	60451	49702	212.193.30.230	192.168.2.3
May 26, 2023 09:30:42.178509951 CEST	49702	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:42.357367992 CEST	60451	49702	212.193.30.230	192.168.2.3
May 26, 2023 09:30:46.512711048 CEST	49703	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:46.731578112 CEST	60451	49703	212.193.30.230	192.168.2.3
May 26, 2023 09:30:47.241487026 CEST	49703	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:47.450041056 CEST	60451	49703	212.193.30.230	192.168.2.3
May 26, 2023 09:30:47.960237026 CEST	49703	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:48.156414986 CEST	60451	49703	212.193.30.230	192.168.2.3
May 26, 2023 09:30:52.262139082 CEST	49704	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:52.470011950 CEST	60451	49704	212.193.30.230	192.168.2.3
May 26, 2023 09:30:52.976330996 CEST	49704	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:53.196007013 CEST	60451	49704	212.193.30.230	192.168.2.3
May 26, 2023 09:30:53.710804939 CEST	49704	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:30:53.921904087 CEST	60451	49704	212.193.30.230	192.168.2.3
May 26, 2023 09:30:58.733969927 CEST	49705	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:59.248977900 CEST	60451	49705	192.169.69.26	192.168.2.3
May 26, 2023 09:30:59.249242067 CEST	49705	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:59.250022888 CEST	49705	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:30:59.750202894 CEST	60451	49705	192.169.69.26	192.168.2.3
May 26, 2023 09:31:04.323385000 CEST	49706	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:04.759567976 CEST	60451	49706	192.169.69.26	192.168.2.3
May 26, 2023 09:31:04.759752035 CEST	49706	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:04.760371923 CEST	49706	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:05.252841949 CEST	60451	49706	192.169.69.26	192.168.2.3
May 26, 2023 09:31:09.356288910 CEST	49707	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:09.761302948 CEST	60451	49707	192.169.69.26	192.168.2.3
May 26, 2023 09:31:09.762080908 CEST	49707	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:09.762080908 CEST	49707	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:10.256534100 CEST	60451	49707	192.169.69.26	192.168.2.3
May 26, 2023 09:31:14.829642057 CEST	49708	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:15.204277039 CEST	60451	49708	212.193.30.230	192.168.2.3
May 26, 2023 09:31:15.712672949 CEST	49708	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:15.955888033 CEST	60451	49708	212.193.30.230	192.168.2.3
May 26, 2023 09:31:16.462724924 CEST	49708	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:16.782919884 CEST	60451	49708	212.193.30.230	192.168.2.3
May 26, 2023 09:31:21.422700882 CEST	49709	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:21.712985992 CEST	60451	49709	212.193.30.230	192.168.2.3
May 26, 2023 09:31:22.228986025 CEST	49709	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:22.448625088 CEST	60451	49709	212.193.30.230	192.168.2.3
May 26, 2023 09:31:22.963390112 CEST	49709	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:23.193901062 CEST	60451	49709	212.193.30.230	192.168.2.3
May 26, 2023 09:31:27.329926968 CEST	49710	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:27.561769009 CEST	60451	49710	212.193.30.230	192.168.2.3
May 26, 2023 09:31:28.073050022 CEST	49710	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:28.373563051 CEST	60451	49710	212.193.30.230	192.168.2.3
May 26, 2023 09:31:28.885606050 CEST	49710	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:29.136476040 CEST	60451	49710	212.193.30.230	192.168.2.3
May 26, 2023 09:31:34.008666039 CEST	49711	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:34.267311096 CEST	60451	49711	192.169.69.26	192.168.2.3
May 26, 2023 09:31:34.267445087 CEST	49711	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:34.268145084 CEST	49711	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:34.752247095 CEST	60451	49711	192.169.69.26	192.168.2.3
May 26, 2023 09:31:39.140110970 CEST	49712	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:39.742539883 CEST	60451	49712	192.169.69.26	192.168.2.3
May 26, 2023 09:31:39.742714882 CEST	49712	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:39.755173922 CEST	49712	60451	192.168.2.3	192.169.69.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 09:31:40.250447989 CEST	60451	49712	192.169.69.26	192.168.2.3
May 26, 2023 09:31:44.892985106 CEST	49713	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:45.262101889 CEST	60451	49713	192.169.69.26	192.168.2.3
May 26, 2023 09:31:45.262805939 CEST	49713	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:45.263535976 CEST	49713	60451	192.168.2.3	192.169.69.26
May 26, 2023 09:31:45.755920887 CEST	60451	49713	192.169.69.26	192.168.2.3
May 26, 2023 09:31:51.904215097 CEST	49714	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:52.107399940 CEST	60451	49714	212.193.30.230	192.168.2.3
May 26, 2023 09:31:52.608714104 CEST	49714	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:52.828514099 CEST	60451	49714	212.193.30.230	192.168.2.3
May 26, 2023 09:31:53.343138933 CEST	49714	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:53.550514936 CEST	60451	49714	212.193.30.230	192.168.2.3
May 26, 2023 09:31:57.937937021 CEST	49715	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:58.185499907 CEST	60451	49715	212.193.30.230	192.168.2.3
May 26, 2023 09:31:58.687335968 CEST	49715	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:58.918368101 CEST	60451	49715	212.193.30.230	192.168.2.3
May 26, 2023 09:31:59.421833038 CEST	49715	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:31:59.642385006 CEST	60451	49715	212.193.30.230	192.168.2.3
May 26, 2023 09:32:03.706192017 CEST	49716	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:32:03.927897930 CEST	60451	49716	212.193.30.230	192.168.2.3
May 26, 2023 09:32:04.437803984 CEST	49716	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:32:04.644476891 CEST	60451	49716	212.193.30.230	192.168.2.3
May 26, 2023 09:32:05.156653881 CEST	49716	60451	192.168.2.3	212.193.30.230
May 26, 2023 09:32:05.390609026 CEST	60451	49716	212.193.30.230	192.168.2.3
May 26, 2023 09:32:10.799665928 CEST	49717	60451	192.168.2.3	192.169.69.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 09:30:24.501882076 CEST	52387	53	192.168.2.3	8.8.8.8
May 26, 2023 09:30:24.615561962 CEST	53	52387	8.8.8.8	192.168.2.3
May 26, 2023 09:30:30.323267937 CEST	56924	53	192.168.2.3	8.8.8.8
May 26, 2023 09:30:30.445596933 CEST	53	56924	8.8.8.8	192.168.2.3
May 26, 2023 09:30:35.382759094 CEST	60625	53	192.168.2.3	8.8.8.8
May 26, 2023 09:30:35.406225920 CEST	53	60625	8.8.8.8	192.168.2.3
May 26, 2023 09:30:40.344777107 CEST	49302	53	192.168.2.3	8.8.8.8
May 26, 2023 09:30:40.379232883 CEST	53	49302	8.8.8.8	192.168.2.3
May 26, 2023 09:30:46.474021912 CEST	53975	53	192.168.2.3	8.8.8.8
May 26, 2023 09:30:46.511017084 CEST	53	53975	8.8.8.8	192.168.2.3
May 26, 2023 09:30:52.229507923 CEST	51139	53	192.168.2.3	8.8.8.8
May 26, 2023 09:30:52.255635023 CEST	53	51139	8.8.8.8	192.168.2.3
May 26, 2023 09:30:58.618963003 CEST	52955	53	192.168.2.3	8.8.8.8
May 26, 2023 09:30:58.731432915 CEST	53	52955	8.8.8.8	192.168.2.3
May 26, 2023 09:31:04.198656082 CEST	60582	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:04.321104050 CEST	53	60582	8.8.8.8	192.168.2.3
May 26, 2023 09:31:09.334753036 CEST	57134	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:09.354583025 CEST	53	57134	8.8.8.8	192.168.2.3
May 26, 2023 09:31:14.642853022 CEST	62050	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:14.671478033 CEST	53	62050	8.8.8.8	192.168.2.3
May 26, 2023 09:31:21.394047976 CEST	56042	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:21.420707941 CEST	53	56042	8.8.8.8	192.168.2.3
May 26, 2023 09:31:27.298899889 CEST	59636	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:27.327780962 CEST	53	59636	8.8.8.8	192.168.2.3
May 26, 2023 09:31:33.882709980 CEST	55638	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:34.004117012 CEST	53	55638	8.8.8.8	192.168.2.3
May 26, 2023 09:31:38.819503069 CEST	57704	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:38.933307886 CEST	53	57704	8.8.8.8	192.168.2.3
May 26, 2023 09:31:44.862737894 CEST	65320	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:44.891343117 CEST	53	65320	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 09:31:51.873344898 CEST	60767	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:51.902283907 CEST	53	60767	8.8.8.8	192.168.2.3
May 26, 2023 09:31:57.900551081 CEST	65107	53	192.168.2.3	8.8.8.8
May 26, 2023 09:31:57.936043978 CEST	53	65107	8.8.8.8	192.168.2.3
May 26, 2023 09:32:03.683854103 CEST	53848	53	192.168.2.3	8.8.8.8
May 26, 2023 09:32:03.704530001 CEST	53	53848	8.8.8.8	192.168.2.3
May 26, 2023 09:32:09.667361975 CEST	57571	53	192.168.2.3	8.8.8.8
May 26, 2023 09:32:09.695261002 CEST	53	57571	8.8.8.8	192.168.2.3
May 26, 2023 09:32:16.277008057 CEST	58691	53	192.168.2.3	8.8.8.8
May 26, 2023 09:32:17.352468014 CEST	58691	53	192.168.2.3	8.8.8.8
May 26, 2023 09:32:17.817212105 CEST	53	58691	8.8.8.8	192.168.2.3
May 26, 2023 09:32:17.817364931 CEST	53	58691	8.8.8.8	192.168.2.3
May 26, 2023 09:32:22.778075933 CEST	53305	53	192.168.2.3	8.8.8.8
May 26, 2023 09:32:22.900695086 CEST	53	53305	8.8.8.8	192.168.2.3

DNS Queries

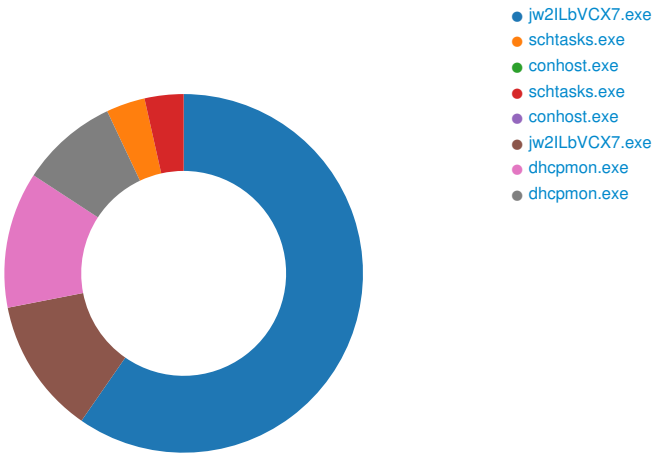
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 09:30:24.501882076 CEST	192.168.2.3	8.8.8.8	0x85ab	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:30.323267937 CEST	192.168.2.3	8.8.8.8	0x3dd9	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:35.382759094 CEST	192.168.2.3	8.8.8.8	0xac83	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:40.344777107 CEST	192.168.2.3	8.8.8.8	0xf519	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:46.474021912 CEST	192.168.2.3	8.8.8.8	0x83a1	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:52.229507923 CEST	192.168.2.3	8.8.8.8	0xbdfc	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:58.618963003 CEST	192.168.2.3	8.8.8.8	0xb7ee	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:04.198656082 CEST	192.168.2.3	8.8.8.8	0x8c29	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:09.334753036 CEST	192.168.2.3	8.8.8.8	0x8855	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:14.642853022 CEST	192.168.2.3	8.8.8.8	0x4900	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:21.394047976 CEST	192.168.2.3	8.8.8.8	0x85b9	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:27.298899889 CEST	192.168.2.3	8.8.8.8	0x7fdd	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:33.882709980 CEST	192.168.2.3	8.8.8.8	0x227b	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:38.819503069 CEST	192.168.2.3	8.8.8.8	0xcbb8	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:44.862737894 CEST	192.168.2.3	8.8.8.8	0x6712	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:51.873344898 CEST	192.168.2.3	8.8.8.8	0x4fc7	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:57.900551081 CEST	192.168.2.3	8.8.8.8	0xd023	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:03.683854103 CEST	192.168.2.3	8.8.8.8	0xe83c	Standard query (0)	december2n d.ddns.net	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:09.667361975 CEST	192.168.2.3	8.8.8.8	0x7eb1	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:16.277008057 CEST	192.168.2.3	8.8.8.8	0x3bdf	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:17.352468014 CEST	192.168.2.3	8.8.8.8	0x3bdf	Standard query (0)	december2n .duckdns.org	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:22.778075933 CEST	192.168.2.3	8.8.8.8	0x14c4	Standard query (0)	december2n .duckdns.org	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 26, 2023 09:30:24.615561962 CEST	8.8.8.8	192.168.2.3	0x85ab	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:30.445596933 CEST	8.8.8.8	192.168.2.3	0x3dd9	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:35.406225920 CEST	8.8.8.8	192.168.2.3	0xac83	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:40.379232883 CEST	8.8.8.8	192.168.2.3	0xf519	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:46.511017084 CEST	8.8.8.8	192.168.2.3	0x83a1	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:52.255635023 CEST	8.8.8.8	192.168.2.3	0xbdfc	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:30:58.731432915 CEST	8.8.8.8	192.168.2.3	0xb7ee	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:04.321104050 CEST	8.8.8.8	192.168.2.3	0x8c29	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:09.354583025 CEST	8.8.8.8	192.168.2.3	0x8855	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:14.671478033 CEST	8.8.8.8	192.168.2.3	0x4900	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:21.420707941 CEST	8.8.8.8	192.168.2.3	0x85b9	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:27.327780962 CEST	8.8.8.8	192.168.2.3	0x7fdd	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:34.004117012 CEST	8.8.8.8	192.168.2.3	0x227b	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:38.933307886 CEST	8.8.8.8	192.168.2.3	0xcbb8	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:44.891343117 CEST	8.8.8.8	192.168.2.3	0x6712	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:51.902283907 CEST	8.8.8.8	192.168.2.3	0x4fc7	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:31:57.936043978 CEST	8.8.8.8	192.168.2.3	0xd023	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:03.704530001 CEST	8.8.8.8	192.168.2.3	0xe83c	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:09.695261002 CEST	8.8.8.8	192.168.2.3	0x7eb1	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:17.817212105 CEST	8.8.8.8	192.168.2.3	0x3bdf	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:17.817364931 CEST	8.8.8.8	192.168.2.3	0x3bdf	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 26, 2023 09:32:22.900695086 CEST	8.8.8.8	192.168.2.3	0x14c4	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: jw2lLbVCX7.exe PID: **6980**, Parent PID: **3452**

General	
Target ID:	0
Start time:	09:30:22
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\jw2lLbVCX7.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\jw2lLbVCX7.exe
Imagebase:	0x670000
File size:	215040 bytes
MD5 hash:	BECA1CB2EAD4D465A208217AC1B189D1
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: 00000000.00000002.645832197.0000000005930000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.645832197.0000000005930000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.645832197.0000000005930000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.645832197.0000000005930000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.368834831.0000000000672000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.368834831.0000000000672000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.368834831.0000000000672000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000000.368834831.0000000000672000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.645656923.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.645656923.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.645656923.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.645656923.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.645871360.0000000005940000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.645871360.0000000005940000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.645871360.0000000005940000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.645871360.0000000005940000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.645871360.0000000005940000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.637063584.0000000002DA1000.00000004.00000800.00020000.00000000.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	6C6660AC	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	6C6660AC	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	4F60D15	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	4F60E0F	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	4F60D15	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4F61094	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	4F61094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpDC9A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4F61290	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4F60E0F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpDDF3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4F61290	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	4F60D15	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	4F60D15	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C6660AC	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	6C6660AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDC9A.tmp	success or wait	1	C4BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpDDF3.tmp	success or wait	1	C4BF0E	DeleteFileW
C:\Users\user\Desktop\jw2ILbVCX7.exe:Zone.Identifier	success or wait	1	4F61625	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	2e 24 fd fd 06 5e fd 48	.$^H	success or wait	1	4F60FC7	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 7e 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 50 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'T~ P	success or wait	2	4F61094	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	4F61094	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDC9A.tmp	0	1300	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	4F60FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	37	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 6a 77 32 49 4c 62 56 43 58 37 2e 65 78 65	C:\Users\user\Desktop\jw2ILbVCX7.exe	success or wait	1	4F60FC7	WriteFile
C:\Users\user\AppData\Local\Temp\tmpDDF3.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	4F60FC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C698738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6C73BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6C73BF06	unknown
C:\Users\user\Desktop\jw2ILbVCX7.exe	unknown	4096	success or wait	1	6C73BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\jw2ILbVCX7.exe	unknown	512	success or wait	1	6C73BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4F60FC7	ReadFile

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	4F61186	RegSetValueExW

Analysis Process: schtasks.exe PID: **7004**, Parent PID: **6980**

General

Target ID:	1
Start time:	09:30:23
Start date:	26/05/2023
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\tmpDC9A.tmp
Imagebase:	0x20000
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\tmpDC9A.tmp	unknown	2	success or wait	1	2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDC9A.tmp	unknown	1301	success or wait	1	2ABD9	ReadFile

Analysis Process: conhost.exe PID: **7068**, Parent PID: **7004**

General

Target ID:	2
Start time:	09:30:23
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **1004**, Parent PID: **6980**

General

Target ID:	3
Start time:	09:30:23
Start date:	26/05/2023
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\tmpDDF3.tmp
Imagebase:	0x20000
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\tmpDDF3.tmp	unknown	2	success or wait	1	2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDDF3.tmp	unknown	1311	success or wait	1	2ABD9	ReadFile

Analysis Process: conhost.exe PID: **2576**, Parent PID: **1004**

General

Target ID:	4
Start time:	09:30:23
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: jw2ILbVCX7.exe PID: **6112**, Parent PID: **1080**

General

Target ID:	5
Start time:	09:30:23
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\jw2ILbVCX7.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\jw2ILbVCX7.exe 0
Imagebase:	0xa40000
File size:	215040 bytes

MD5 hash:	BECA1CB2EAD4D465A208217AC1B189D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.387696343.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.387696343.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000002.387696343.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.387807727.0000000004041000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.387807727.0000000004041000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000002.387807727.0000000004041000.00000004.00000800.00020000.00000000.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	6C6660AC	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	6C6660AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\jw2ILbVCX7.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C6534A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\jw2ILbVCX7.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6C93A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C695544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C698738	ReadFile

Analysis Process: dhcpmon.exe PID: **5748**, Parent PID: **1080**

General

Target ID:	6
Start time:	09:30:23
Start date:	26/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x210000
File size:	215040 bytes
MD5 hash:	BECA1CB2EAD4D465A208217AC1B189D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.388017452.0000000002831000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.388017452.0000000002831000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.388017452.0000000002831000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 97%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C6660AC	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	6C6660AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C6534A7	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_v2.0_32\UsageLogs\dhcpmon.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6C93A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C698738	ReadFile

Analysis Process: dhcpmon.exe PID: **7076**, Parent PID: **3452**

General

Target ID:	7
Start time:	09:30:31
Start date:	26/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xd50000
File size:	215040 bytes
MD5 hash:	BECA1CB2EAD4D465A208217AC1B189D1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C6660AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C6660AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C695544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C698738	ReadFile

Disassembly

No disassembly