ID: 624876
Sample Name: 8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
Cookbook: default.jbs
Time: 07:55:26
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

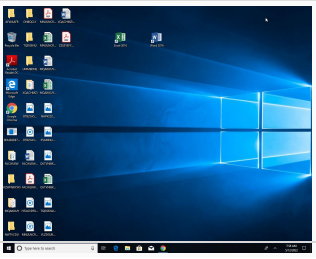
Windows Analysis Report

8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe

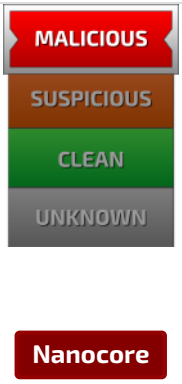
Overview

General Information

Sample Name:	8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
Analysis ID:	624876
MD5:	df1dc1a245d930..
SHA1:	b2f5da6a917d95..
SHA256:	8fa3b2eb7650ac..
Tags:	exe NanoCore RAT
Infos:	



Detection



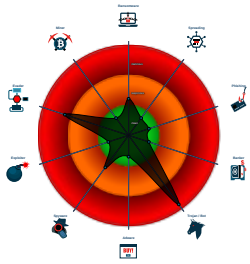
Nanocore

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…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- 8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe (PID: 6408 cmdline: "C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe" MD5: DF1DC1A245D93014003E9ECC4F654602)
  - schtasks.exe (PID: 6448 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp187C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6544 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp21A4.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe (PID: 6536 cmdline: C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe 0 MD5: DF1DC1A245D93014003E9ECC4F654602)
- dhcpmon.exe (PID: 6776 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: DF1DC1A245D93014003E9ECC4F654602)
- dhcpmon.exe (PID: 6860 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: DF1DC1A245D93014003E9ECC4F654602)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "3577d152-ce3c-4012-b95b-9d207c3b",
  "Group": "Default",
  "Domain1": "khalil3131.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 1991,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.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
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.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

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000000.291791981.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000000.291791981.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000009.00000000.291791981.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000003.00000002.298371939.0000000002B01000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000003.00000002.298371939.0000000002B01000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x23ccb:$a: NanoCore • 0x23d24:$a: NanoCore • 0x23d61:$a: NanoCore • 0x23dda:$a: NanoCore • 0x23d2d:$b: ClientPlugin • 0x23d6a:$b: ClientPlugin • 0x24668:$b: ClientPlugin • 0x24675:$b: ClientPlugin • 0x1ba3f:$e: KeepAlive • 0x241b5:$g: LogClientMessage • 0x24135:$i: get_Connected • 0x15cfd:$j: #=q • 0x15d2d:$j: #=q • 0x15d69:$j: #=q • 0x15d91:$j: #=q • 0x15dc1:$j: #=q • 0x15df1:$j: #=q • 0x15e21:$j: #=q • 0x15e51:$j: #=q • 0x15e6d:$j: #=q • 0x15e9d:$j: #=q
Click to see the 51 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.430000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
3.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.430000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
3.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.430000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
3.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.430000.0.unpack	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:$s7: get_Connected
3.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.430000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$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 125 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5 −

Timestamp:	192.168.2.391.109.186.54978519912816766 05/12/22-07:58:38.292297
SID:	2816766

Source Port:	49785
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54974419912025019 05/12/22-07:57:00.726091
SID:	2025019
Source Port:	49744
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54976219912816766 05/12/22-07:57:29.709544
SID:	2816766
Source Port:	49762
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54976519912816766 05/12/22-07:57:45.216192
SID:	2816766
Source Port:	49765
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54974419912816718 05/12/22-07:57:02.037427
SID:	2816718
Source Port:	49744
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54975419912025019 05/12/22-07:57:14.238146
SID:	2025019
Source Port:	49754
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978219912816766 05/12/22-07:58:25.058984
SID:	2816766
Source Port:	49782
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54974519912816766 05/12/22-07:57:09.662455
SID:	2816766
Source Port:	49745
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54977019912816718 05/12/22-07:57:58.710592
SID:	2816718
Source Port:	49770
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978319912025019 05/12/22-07:58:29.840228
SID:	2025019
Source Port:	49783
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 91.109.186.5 - Destination IP: 192.168.2.3	
Timestamp:	91.109.186.5192.168.2.31991497702810290 05/12/22-07:57:57.386403
SID:	2810290
Source Port:	1991
Destination Port:	49770
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978619912816766 05/12/22-07:58:44.794630
SID:	2816766
Source Port:	49786
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54974519912025019 05/12/22-07:57:07.733942
SID:	2025019
Source Port:	49745
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54977319912816766 05/12/22-07:58:03.947984
SID:	2816766
Source Port:	49773
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54975419912816766 05/12/22-07:57:16.743146
SID:	2816766
Source Port:	49754
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54976419912025019 05/12/22-07:57:35.770968
SID:	2025019
Source Port:	49764

Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	−
Timestamp:	192.168.2.391.109.186.54977019912025019 05/12/22-07:57:57.148651
SID:	2025019
Source Port:	49770
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	−
Timestamp:	192.168.2.391.109.186.54974419912816766 05/12/22-07:57:02.725769
SID:	2816766
Source Port:	49744
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	−
Timestamp:	192.168.2.391.109.186.54978019912025019 05/12/22-07:58:16.673778
SID:	2025019
Source Port:	49780
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	−
Timestamp:	192.168.2.391.109.186.54978319912816766 05/12/22-07:58:31.726985
SID:	2816766
Source Port:	49783
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	−
Timestamp:	192.168.2.391.109.186.54977419912025019 05/12/22-07:58:08.550021
SID:	2025019
Source Port:	49774
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	−
Timestamp:	192.168.2.391.109.186.54977019912816766 05/12/22-07:57:58.935372
SID:	2816766
Source Port:	49770
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	−
Timestamp:	192.168.2.391.109.186.54976219912025019 05/12/22-07:57:27.823235
SID:	2025019
Source Port:	49762
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978919912025019 05/12/22-07:58:49.123054
SID:	2025019
Source Port:	49789
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54976419912816766 05/12/22-07:57:38.690881
SID:	2816766
Source Port:	49764
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54976519912025019 05/12/22-07:57:43.204061
SID:	2025019
Source Port:	49765
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978519912025019 05/12/22-07:58:36.405902
SID:	2025019
Source Port:	49785
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54977419912816766 05/12/22-07:58:10.389760
SID:	2816766
Source Port:	49774
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54974319912816766 05/12/22-07:56:52.560880
SID:	2816766
Source Port:	49743
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978019912816766 05/12/22-07:58:18.415033
SID:	2816766
Source Port:	49780
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54974319912025019 05/12/22-07:56:50.755839
SID:	2025019
Source Port:	49743

Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54976619912816766 05/12/22-07:57:51.591169
SID:	2816766
Source Port:	49766
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978619912025019 05/12/22-07:58:42.971078
SID:	2025019
Source Port:	49786
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54975619912816766 05/12/22-07:57:23.127316
SID:	2816766
Source Port:	49756
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54975619912025019 05/12/22-07:57:21.352785
SID:	2025019
Source Port:	49756
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54976619912025019 05/12/22-07:57:49.806421
SID:	2025019
Source Port:	49766
Destination Port:	1991
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 91.109.186.5	
Timestamp:	192.168.2.391.109.186.54978219912025019 05/12/22-07:58:23.335512
SID:	2025019
Source Port:	49782
Destination Port:	1991
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

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

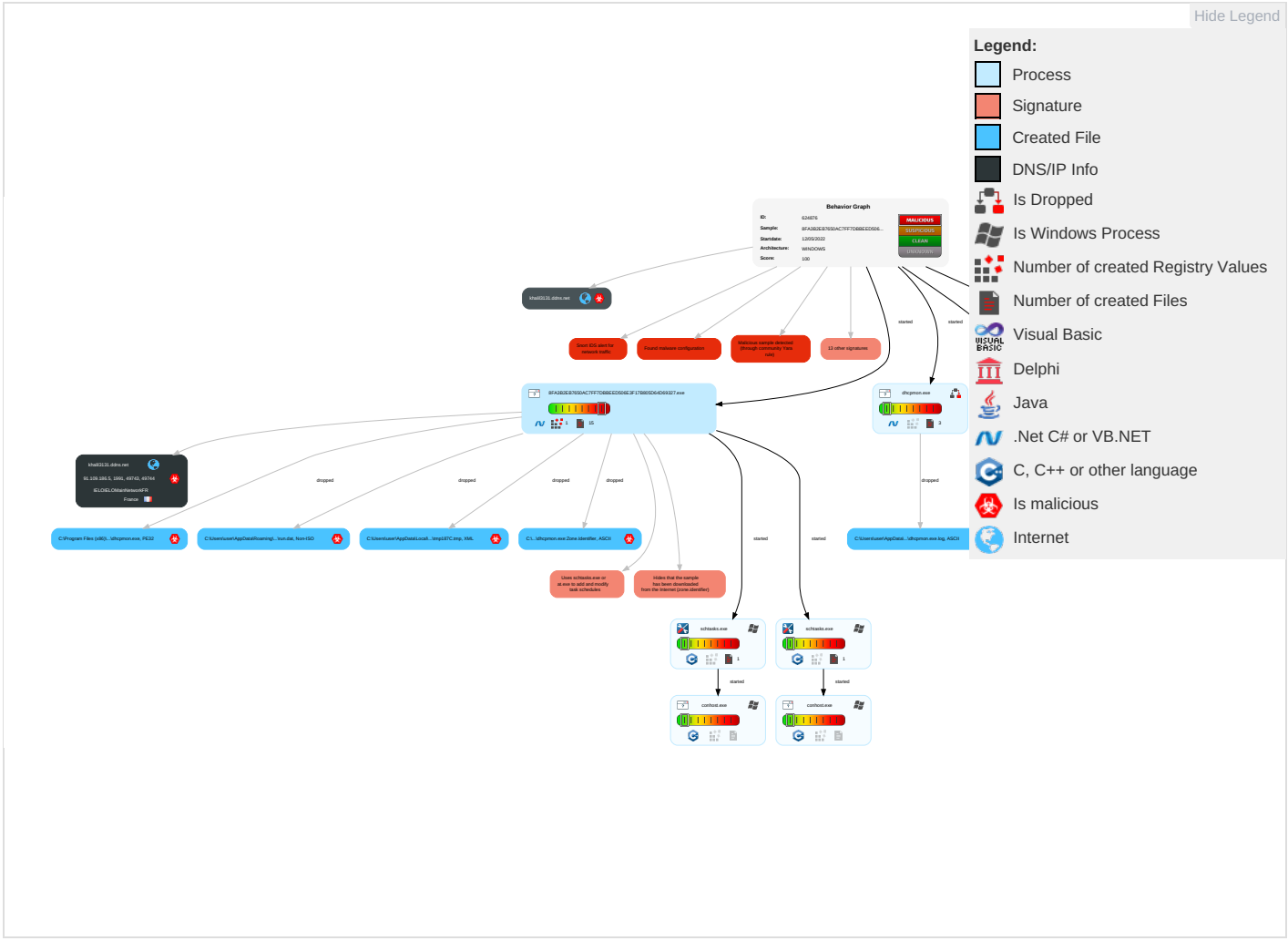
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 Access Token Manipulation	2 Masquerading	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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	3 System Information 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	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

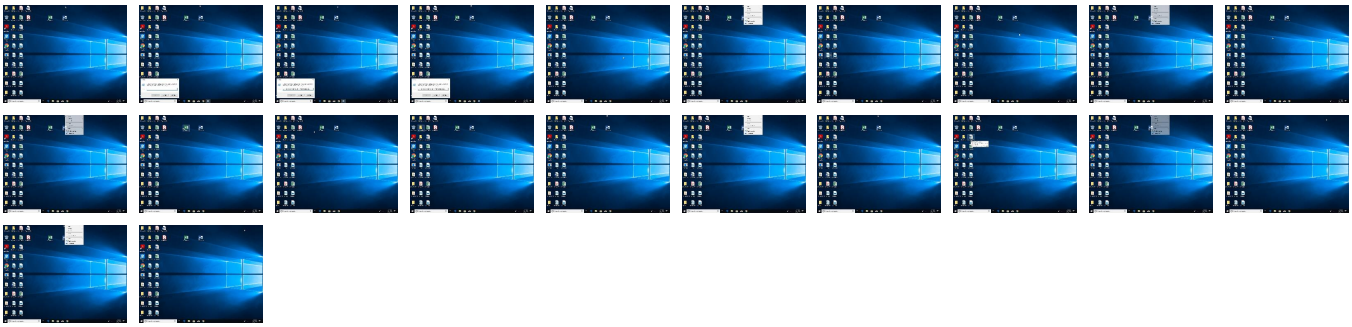
Behavior Graph



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
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	86%	Virustotal		Browse
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	86%	Metadefender		Browse
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.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		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	86%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.44e7ab0.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File
3.0.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.430000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.dhcpmon.exe.db0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.dhcpmon.exe.d0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.430000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.dhcpmon.exe.d0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.ca0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.ca0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.5f80000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.0.dhcpmon.exe.db0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
khalil3131.ddns.net	100%	Avira URL Cloud	malware	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

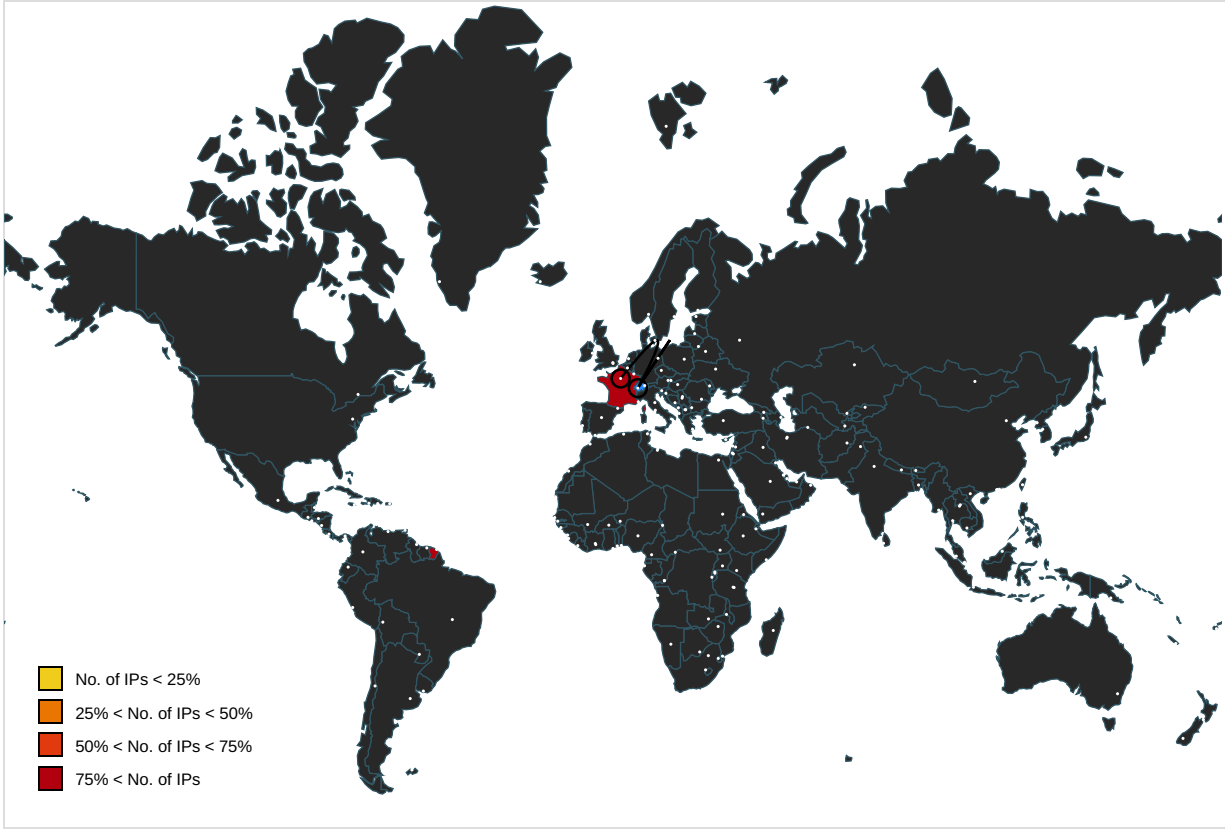
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
khalil3131.ddns.net	91.109.186.5	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
khalil3131.ddns.net	true	• Avira URL Cloud: malware	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.109.186.5	khalil3131.ddns.net	France		29075	IELOIELOMainNetworkFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624876
Start date and time: 12/05/202207:55:26	2022-05-12 07:55:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/9@18/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.152.110.14, 40.125.122.176, 52.242.101.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:56:43	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
07:56:46	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe" s>$(Arg0)
07:56:49	API Interceptor	889x Sleep call for process: 8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe modified
07:56:50	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

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\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

Size (bytes):	207872
Entropy (8bit):	7.449716258096661
Encrypted:	false
SSDEEP:	3072:szEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIXJPAGTwjgaxODOeSQcY/UShKT:sLV6Bta6dtJmakIM5Ir8PxtPY/1KT
MD5:	DF1DC1A245D93014003E9ECC4F654602
SHA1:	B2F5DA6A917D9535A623DE61C603D03F0D225FB4
SHA-256:	8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D6932715F8885508FB6F988C6
SHA-512:	05E6AF5EA0218F3FA03782437373B68A00E95CD9BC9D90FB36E1575D09C964019B7D54CD57246A0B843E2666AC1338197227B613B6FDCF1963F2A364B508A2C7
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 • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • 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>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 98%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....8...W.... ..._..... ....H.....text..... ....`.reloc.....@..B.rsrc...._... ...`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&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\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.log

Process:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.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**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

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

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

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

C:\Users\user\AppData\Local\Temp\tmp187C.tmp

Process:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1335
Entropy (8bit):	5.213341096764609
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0EIy3xtn:cbk4oL600QydbQxIYODOLedq3J3j
MD5:	0A1F07A06540020B73F62710794160BD
SHA1:	9063FD28DD342A6640746A3D797F1D9FE63B291D
SHA-256:	0C48FB31BC2830791F55EED4BDFE7D63D6A25F13992F45B501E0572DD386C875
SHA-512:	7ECDA872E34779ED83D808AB998D803DEC209E8C87D04A858960ECDFD5650B49D213CC1C1A11615AAFF2CBA54AFEE005CE9AADE5DA486CC6BC751433634B03B
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\tmp21A4.tmp

Process:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File Type:	data
Category:	modified

Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&

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

Process:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:9Sl:9s
MD5:	1DE95590512455690E9C4A8ECD7205E4
SHA1:	C328665D12D5A6291B465792573BD8E3BEF209AD
SHA-256:	6F905D8CEA028A5E82059798F92A7CDAD70D47ACE17D101FC9487DCE33466D4D
SHA-512:	59D9372193DE6B0DBA93596D43492E5652CC6AFA1488F0BF0CAA2A1DBE994BC0DB606BD68B7894D828D20D0F8F62957BA3C86731A79767465FA303F23142FBF
Malicious:	**true**
Preview:	....'4.H

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

Process:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.727585120442808
Encrypted:	false
SSDEEP:	3:oNWXp5vdjkTWSnnggh216d4N:oNWXpF3Unggh54
MD5:	591AEF748C8D2CA5AEC3419BDE1BD8FF
SHA1:	660EC4B1ECCF185F68113A52CA4CF7AC79B614B4
SHA-256:	FE23408EB733D1F845D83D6D2972934FEEF1C0097C7FAB221AD4F41E21523293
SHA-512:	96061B47BEC49B1575FDF414F332D0CBDD6CB3B089E56F1968B03F69839D25CA22CE4EFC96CC7AB42D9B4CCF7F13ACC7ECA38F828D92C7CF806A598684B88FB
Malicious:	false
Preview:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.449716258096661
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:	8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
File size:	207872
MD5:	df1dc1a245d93014003e9ecc4f654602
SHA1:	b2f5da6a917d9535a623de61c603d03f0d225fb4
SHA256:	8fa3b2eb7650ac7ff7dbbeed506e3f17b805d64d6932715f8885508fb6f988c6

SHA512:	05e6af5ea0218f3fa03782437373b68a00e95cd9bc9d90fb36e1575d09c964019b7d54cd57246a0b843e2666ac1338197227b613b6fdcf1963f2a364b508a2c7
SSDEEP:	3072:szEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIXJPAGTwjgaxODOeSQcY/UShKT:sLV6Bta6dtJmakIM5Ir8PxtPY/1KT
TLSH:	4C14CF563BE98A3ED2DF85B8611202578378C2E7D9D3F3DA18D851B78B627E40A070D7
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....'.T.....................b........... ....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

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

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

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	0x15fc8	.rsrc
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	0.594503837719	data	6.59804476018	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15fc8	0x16000	False	1.00031072443	data	7.99780343549	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x15f70	TIM image, Pixel at (10392,19457) Size=2043x65115		

Imports

DLL	Import
mscoree.dll	_CorExeMain

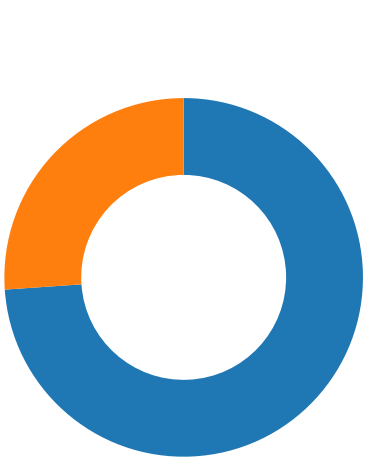
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.391.109.186.54 978519912816766 05/12/22-07:58:38.292297	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49785	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 974419912025019 05/12/22-07:57:00.726091	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976219912816766 05/12/22-07:57:29.709544	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49762	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976519912816766 05/12/22-07:57:45.216192	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49765	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 974419912816718 05/12/22-07:57:02.037427	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49744	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 975419912025019 05/12/22-07:57:14.238146	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978219912816766 05/12/22-07:58:25.058984	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49782	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 974519912816766 05/12/22-07:57:09.662455	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49745	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 977019912816718 05/12/22-07:57:58.710592	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49770	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978319912025019 05/12/22-07:58:29.840228	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	1991	192.168.2.3	91.109.186.5
91.109.186.5192.168.2.31 991497702810290 05/12/22-07:57:57.386403	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1991	49770	91.109.186.5	192.168.2.3
192.168.2.391.109.186.54 978619912816766 05/12/22-07:58:44.794630	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49786	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 974519912025019 05/12/22-07:57:07.733942	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 977319912816766 05/12/22-07:58:03.947984	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49773	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 975419912816766 05/12/22-07:57:16.743146	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49754	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976419912025019 05/12/22-07:57:35.770968	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 977019912025019 05/12/22-07:57:57.148651	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 974419912816766 05/12/22-07:57:02.725769	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49744	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978019912025019 05/12/22-07:58:16.673778	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	1991	192.168.2.3	91.109.186.5

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.391.109.186.54 978319912816766 05/12/22-07:58:31.726985	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49783	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 977419912025019 05/12/22-07:58:08.550021	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 977019912816766 05/12/22-07:57:58.935372	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49770	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976219912025019 05/12/22-07:57:27.823235	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978919912025019 05/12/22-07:58:49.123054	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976419912816766 05/12/22-07:57:38.690881	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49764	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976519912025019 05/12/22-07:57:43.204061	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978519912025019 05/12/22-07:58:36.405902	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 977419912816766 05/12/22-07:58:10.389760	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49774	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 974319912816766 05/12/22-07:56:52.560880	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49743	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978019912816766 05/12/22-07:58:18.415033	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49780	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 974319912025019 05/12/22-07:56:50.755839	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976619912816766 05/12/22-07:57:51.591169	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49766	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978619912025019 05/12/22-07:58:42.971078	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 975619912816766 05/12/22-07:57:23.127316	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49756	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 975619912025019 05/12/22-07:57:21.352785	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 976619912025019 05/12/22-07:57:49.806421	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	1991	192.168.2.3	91.109.186.5
192.168.2.391.109.186.54 978219912025019 05/12/22-07:58:23.335512	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	1991	192.168.2.3	91.109.186.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 07:56:50.539573908 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:50.668284893 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:50.668468952 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:50.755839109 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:51.017306089 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:51.017383099 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:51.303261995 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:51.303349972 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:51.509748936 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:51.586275101 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:51.586765051 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:51.637226105 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:51.644325972 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:51.757510900 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:51.918226957 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:51.920588970 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.247191906 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.247437954 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.292334080 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.292467117 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.307349920 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.307497978 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.321219921 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.321297884 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.336314917 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.336502075 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.350361109 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.350434065 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.365328074 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.365421057 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.379390955 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.379463911 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.394315004 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.394382000 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.408458948 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.408603907 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.423321009 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.423480988 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.560709953 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.560879946 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.574340105 CEST	1991	49743	91.109.186.5	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 07:56:52.574445009 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.589399099 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.589541912 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.603425026 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.603625059 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.618385077 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.618510008 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.632329941 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.632508039 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.639597893 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.647301912 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.647418022 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.661343098 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.661408901 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.676328897 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.676493883 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.690356970 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.690505028 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.705364943 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.705516100 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.719393015 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.719518900 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.734338045 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.734464884 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.748327971 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.748451948 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.763458967 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.763600111 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.777298927 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.777380943 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.794317007 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.794421911 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.808258057 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.808419943 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.823251963 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.823363066 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.837270021 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.837399006 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.855340958 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.855494022 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.870321989 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.870464087 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.884305000 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.884403944 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.899338007 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.899445057 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.913316965 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.913398027 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.928405046 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.928531885 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.942298889 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.942693949 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.957298994 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.957470894 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.971311092 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.971438885 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:52.986308098 CEST	1991	49743	91.109.186.5	192.168.2.3
May 12, 2022 07:56:52.986397028 CEST	49743	1991	192.168.2.3	91.109.186.5
May 12, 2022 07:56:53.000297070 CEST	1991	49743	91.109.186.5	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 07:56:50.503297091 CEST	64851	53	192.168.2.3	8.8.8.8
May 12, 2022 07:56:50.524601936 CEST	53	64851	8.8.8.8	192.168.2.3
May 12, 2022 07:57:00.567784071 CEST	49316	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:00.590230942 CEST	53	49316	8.8.8.8	192.168.2.3
May 12, 2022 07:57:07.568006992 CEST	56417	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:07.587565899 CEST	53	56417	8.8.8.8	192.168.2.3
May 12, 2022 07:57:14.085995913 CEST	57421	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:14.105559111 CEST	53	57421	8.8.8.8	192.168.2.3
May 12, 2022 07:57:21.200678110 CEST	49873	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:21.221888065 CEST	53	49873	8.8.8.8	192.168.2.3
May 12, 2022 07:57:27.661298990 CEST	49327	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:27.682848930 CEST	53	49327	8.8.8.8	192.168.2.3
May 12, 2022 07:57:35.116136074 CEST	58981	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:35.138746023 CEST	53	58981	8.8.8.8	192.168.2.3
May 12, 2022 07:57:43.055500031 CEST	64452	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:43.074953079 CEST	53	64452	8.8.8.8	192.168.2.3
May 12, 2022 07:57:49.621150017 CEST	61380	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:49.643440962 CEST	53	61380	8.8.8.8	192.168.2.3
May 12, 2022 07:57:57.000972986 CEST	52810	53	192.168.2.3	8.8.8.8
May 12, 2022 07:57:57.018244982 CEST	53	52810	8.8.8.8	192.168.2.3
May 12, 2022 07:58:03.777712107 CEST	55151	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:03.795254946 CEST	53	55151	8.8.8.8	192.168.2.3
May 12, 2022 07:58:08.391948938 CEST	59795	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:08.415642977 CEST	53	59795	8.8.8.8	192.168.2.3
May 12, 2022 07:58:16.497291088 CEST	64816	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:16.518326998 CEST	53	64816	8.8.8.8	192.168.2.3
May 12, 2022 07:58:22.992727995 CEST	64996	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:23.013859987 CEST	53	64996	8.8.8.8	192.168.2.3
May 12, 2022 07:58:29.546488047 CEST	53816	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:29.566279888 CEST	53	53816	8.8.8.8	192.168.2.3
May 12, 2022 07:58:36.256527901 CEST	52096	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:36.275990009 CEST	53	52096	8.8.8.8	192.168.2.3
May 12, 2022 07:58:42.822968960 CEST	60640	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:42.840430975 CEST	53	60640	8.8.8.8	192.168.2.3
May 12, 2022 07:58:48.970896959 CEST	63861	53	192.168.2.3	8.8.8.8
May 12, 2022 07:58:48.990263939 CEST	53	63861	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 07:56:50.503297091 CEST	192.168.2.3	8.8.8.8	0xec6d	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:00.567784071 CEST	192.168.2.3	8.8.8.8	0x4057	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:07.568006992 CEST	192.168.2.3	8.8.8.8	0x54a4	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:14.085995913 CEST	192.168.2.3	8.8.8.8	0x4379	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:21.200678110 CEST	192.168.2.3	8.8.8.8	0xfab9	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:27.661298990 CEST	192.168.2.3	8.8.8.8	0x9dc1	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:35.116136074 CEST	192.168.2.3	8.8.8.8	0x64e8	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:43.055500031 CEST	192.168.2.3	8.8.8.8	0x2cca	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:49.621150017 CEST	192.168.2.3	8.8.8.8	0x1545	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:57:57.000972986 CEST	192.168.2.3	8.8.8.8	0x7a8d	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 07:58:03.777712107 CEST	192.168.2.3	8.8.8.8	0x9ba	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:58:08.391948938 CEST	192.168.2.3	8.8.8.8	0x9ae1	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:58:16.497291088 CEST	192.168.2.3	8.8.8.8	0xb2bd	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:58:22.992727995 CEST	192.168.2.3	8.8.8.8	0xaff3	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:58:29.546488047 CEST	192.168.2.3	8.8.8.8	0x4b78	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:58:36.256527901 CEST	192.168.2.3	8.8.8.8	0x79d1	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:58:42.822968960 CEST	192.168.2.3	8.8.8.8	0x9850	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 07:58:48.970896959 CEST	192.168.2.3	8.8.8.8	0x91b7	Standard query (0)	khalil3131 .ddns.net	A (IP address)	IN (0x0001)

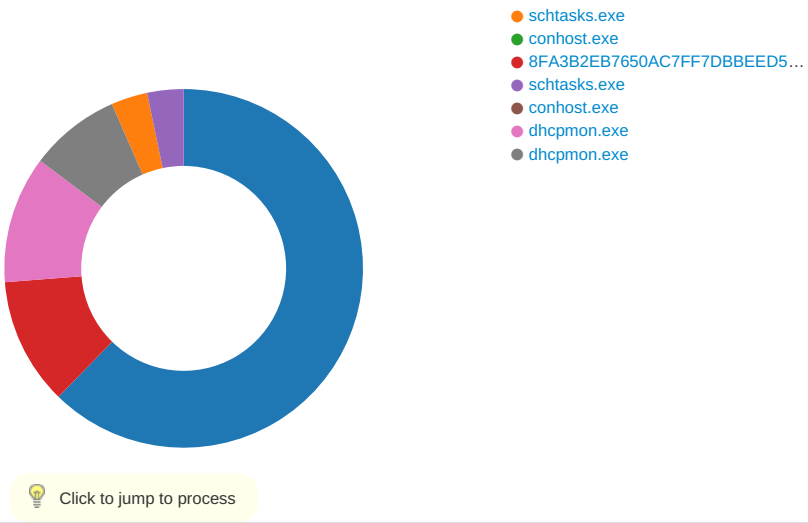
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 07:56:50.524601936 CEST	8.8.8.8	192.168.2.3	0xec6d	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:00.590230942 CEST	8.8.8.8	192.168.2.3	0x4057	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:07.587565899 CEST	8.8.8.8	192.168.2.3	0x54a4	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:14.105559111 CEST	8.8.8.8	192.168.2.3	0x4379	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:21.221888065 CEST	8.8.8.8	192.168.2.3	0xfab9	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:27.682848930 CEST	8.8.8.8	192.168.2.3	0x9dc1	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:35.138746023 CEST	8.8.8.8	192.168.2.3	0x64e8	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:43.074953079 CEST	8.8.8.8	192.168.2.3	0x2cca	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:49.643440962 CEST	8.8.8.8	192.168.2.3	0x1545	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:57:57.018244982 CEST	8.8.8.8	192.168.2.3	0x7a8d	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:03.795254946 CEST	8.8.8.8	192.168.2.3	0x9ba	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:08.415642977 CEST	8.8.8.8	192.168.2.3	0x9ae1	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:16.518326998 CEST	8.8.8.8	192.168.2.3	0xb2bd	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:23.013859987 CEST	8.8.8.8	192.168.2.3	0xaff3	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:29.566279888 CEST	8.8.8.8	192.168.2.3	0x4b78	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:36.275990009 CEST	8.8.8.8	192.168.2.3	0x79d1	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:42.840430975 CEST	8.8.8.8	192.168.2.3	0x9850	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)
May 12, 2022 07:58:48.990263939 CEST	8.8.8.8	192.168.2.3	0x91b7	No error (0)	khalil3131 .ddns.net		91.109.186.5	A (IP address)	IN (0x0001)

Statistics

Behavior

● 8FA3B2EB7650AC7FF7DBBEED5…



System Behavior

Analysis Process: 8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe PID: **6408**, Parent PID: **5844**

General

Target ID:	0
Start time:	07:56:41
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe"
Imagebase:	0xca0000
File size:	207872 bytes
MD5 hash:	DF1DC1A245D93014003E9ECC4F654602
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: 00000000.00000002.545700012.0000000005860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.545700012.0000000005860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.545700012.0000000005860000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.546009139.0000000005F80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.546009139.0000000005F80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.546009139.0000000005F80000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.546009139.0000000005F80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.538786441.0000000000CA2000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.538786441.0000000000CA2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.538786441.0000000000CA2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.271804888.0000000000CA2000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.271804888.0000000000CA2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.271804888.0000000000CA2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.545464811.00000000044DB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	723A60AC	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	723A60AC	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	5590D15	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	5590E0F	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	5590D15	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	5591094	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	5591094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp187C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5591290	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	5590E0F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp21A4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5591290	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	5590D15	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	5590D15	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	723A60AC	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	723A60AC	unknown
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	16	5590E0F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp187C.tmp	success or wait	1	71987D95	unknown
C:\Users\user\AppData\Local\Temp\tmp21A4.tmp	success or wait	1	71987D95	unknown
C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe:Zone.Identifier	success or wait	1	5591625	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	09 fd fd fd 27 34 fd 48	'4H	success or wait	1	5590FC7	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 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 62 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 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'Tb @	success or wait	2	5591094	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	5591094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp187C.tmp	0	1335	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	5590FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	72	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 38 46 41 33 42 32 45 42 37 36 35 30 41 43 37 46 46 37 44 42 42 45 45 44 35 30 36 45 33 46 31 37 42 38 30 35 44 36 34 44 36 39 33 32 37 2e 65 78 65	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	success or wait	1	5590FC7	WriteFile
C:\Users\user\AppData\Local\Temp\tmp21A4.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	5590FC7	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 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb4ht+Z\ iS}FF2hM+L#X+*~fG0^;.W2=K~L&f.p:7rH}/HL?AKJ=8x!+2e'E?G[&	success or wait	13	5590FC7	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	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	723D8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7247BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7247BF06	unknown
C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe	unknown	4096	success or wait	1	7247BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\8FA3B2EB 7650AC7FF7DBBEED506E3F17B805D64D69327.exe	unknown	512	success or wait	1	7247BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	4095	success or wait	1	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	8175	end of file	1	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	4096	end of file	1	5590FC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7247BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7247BF06	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	5591186	RegSetValueExW

Analysis Process: schtasks.exe PID: **6448**, Parent PID: **6408**

General

Target ID:	1
Start time:	07:56:43
Start date:	12/05/2022
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\tmp187C.tmp
Imagebase:	0xb40000
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\tmp187C.tmp	unknown	2	success or wait	1	B4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp187C.tmp	unknown	1336	success or wait	1	B4ABD9	ReadFile

Analysis Process: conhost.exe PID: **6488**, Parent PID: **6448**

General

Target ID:	2
Start time:	07:56:44
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: 8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe PID: **6536**, Parent PID: **848**

General

Target ID:	3
Start time:	07:56:46
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe 0
Imagebase:	0x430000
File size:	207872 bytes
MD5 hash:	DF1DC1A245D93014003E9ECC4F654602
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: 00000003.00000002.298371939.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.298371939.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.282231195.0000000000432000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.282231195.0000000000432000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.282231195.0000000000432000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.297856567.0000000000432000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.297856567.0000000000432000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.297856567.0000000000432000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.298492088.0000000003B01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.298492088.0000000003B01000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	723A60AC	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	723A60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	723934A7	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\8FA3B2EB7650AC7FF7DBBEED506E3F17B805D64D69327.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	7267A33A	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	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	723D8738	ReadFile

Analysis Process: schtasks.exe PID: **6544**, Parent PID: **6408**

General

Target ID:	4
Start time:	07:56:46
Start date:	12/05/2022
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\tmp21A4.tmp
Imagebase:	0xb40000
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\tmp21A4.tmp	unknown	2	success or wait	1	B4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp21A4.tmp	unknown	1311	success or wait	1	B4ABD9	ReadFile

Analysis Process: conhost.exe PID: **6624**, Parent PID: **6544**

General	
Target ID:	6
Start time:	07:56:48
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: **6776**, Parent PID: **848**

General	
Target ID:	9
Start time:	07:56:50
Start date:	12/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xdb0000
File size:	207872 bytes
MD5 hash:	DF1DC1A245D93014003E9ECC4F654602
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: 00000009.00000000.291791981.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.291791981.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.291791981.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.312387842.0000000003461000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.312387842.0000000003461000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.311896346.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.311896346.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.311896346.0000000000DB2000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.312592762.0000000004461000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.312592762.0000000004461000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • 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>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, Metadefender, Browse • Detection: 98%, 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	723A60AC	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	723A60AC	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	723934A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	7267A33A	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	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	723D8738	ReadFile

Analysis Process: dhcpmon.exe PID: **6860**, Parent PID: **3968**

General

Target ID:	11
Start time:	07:56:51
Start date:	12/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xd0000
File size:	207872 bytes
MD5 hash:	DF1DC1A245D93014003E9ECC4F654602
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.294404825.00000000000D2000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.294404825.00000000000D2000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.294404825.00000000000D2000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314675096.0000000002781000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314675096.0000000002781000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.314132529.00000000000D2000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314132529.00000000000D2000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314132529.00000000000D2000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314708127.0000000003781000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314708127.0000000003781000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	723A60AC	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	723A60AC	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	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	723D5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	723D8738	ReadFile

Disassembly

No disassembly