ID: 878709
Sample Name: Quotation Details.exe
Cookbook: default.jbs
Time: 03:55:15
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

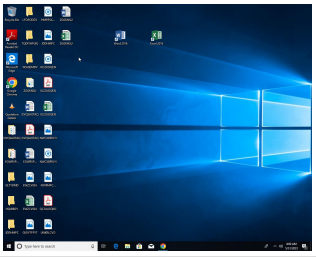
Windows Analysis Report

Quotation Details.exe

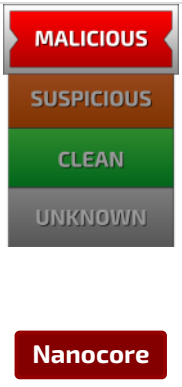
Overview

General Information

Sample Name:	Quotation Details.exe
Analysis ID:	878709
MD5:	5ec7a9d9a56fa…
SHA1:	77719c19c79e…
SHA256:	dee80ff02e834…
Infos:	



Detection



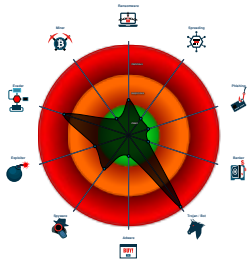
Nanocore

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
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Initial sample is a PE file and has a…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- Quotation Details.exe (PID: 7120 cmdline: C:\Users\user\Desktop\Quotation Details.exe MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
  - Quotation Details.exe (PID: 5328 cmdline: C:\Users\user\Desktop\Quotation Details.exe MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
    - schtasks.exe (PID: 1968 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpE4FD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2108 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpE6C3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Quotation Details.exe (PID: 2600 cmdline: "C:\Users\user\Desktop\Quotation Details.exe" 0 MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
  - Quotation Details.exe (PID: 5356 cmdline: C:\Users\user\Desktop\Quotation Details.exe MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
  - Quotation Details.exe (PID: 5644 cmdline: C:\Users\user\Desktop\Quotation Details.exe MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
- dhcpmon.exe (PID: 1276 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
  - dhcpmon.exe (PID: 2404 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
  - dhcpmon.exe (PID: 2220 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
- dhcpmon.exe (PID: 5692 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
  - dhcpmon.exe (PID: 3616 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 5EC7A9D9A56FA3EB2D6F63A555969A37)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "0d867adb-3500-4c95-b576-70e197aa",
  "Group": "UC1",
  "Domain1": "ucnano180523.ddns.net",
  "Domain2": "ucnano180523.ddns.net",
  "Port": 5899,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.622362871.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000D.00000002.622362871.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x69463:$a: NanoCore • 0x694bc:$a: NanoCore • 0x694f9:$a: NanoCore • 0x69572:$a: NanoCore • 0x694c5:$b: ClientPlugin • 0x69502:$b: ClientPlugin • 0x69e00:$b: ClientPlugin • 0x69e0d:$b: ClientPlugin • 0x5f5e5:$e: KeepAlive • 0x6994d:$g: LogClientMessage • 0x698cd:$i: get_Connected • 0x59899:$j: #=q • 0x598c9:$j: #=q • 0x59905:$j: #=q • 0x5992d:$j: #=q • 0x5995d:$j: #=q • 0x5998d:$j: #=q • 0x599bd:$j: #=q • 0x599ed:$j: #=q • 0x59a09:$j: #=q • 0x59a39:$j: #=q
0000000D.00000002.622362871.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x694f9:$a1: NanoCore.ClientPluginHost • 0x694bc:$a2: NanoCore.ClientPlugin • 0x5add3:$b1: get_BuilderSettings • 0x69890:$b1: get_BuilderSettings • 0x69547:$b4: IClientAppHost • 0x69901:$b6: AddHostEntry • 0x5ad42:$b7: LogClientException • 0x69970:$b7: LogClientException • 0x698e5:$b8: PipeExists • 0x69534:$b9: IClientLoggingHost
00000003.00000003.578596362.0000000001511000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x49ac:$a1: NanoCore.ClientPluginHost • 0x4987:$a2: NanoCore.ClientPlugin • 0x499d:$b4: IClientAppHost • 0x8e8c:$b7: LogClientException • 0x49d6:$b9: IClientLoggingHost
00000001.00000002.565244380.000000000416B000.00000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x47e4d:$x1: NanoCore.ClientPluginHost • 0x7aa6d:$x1: NanoCore.ClientPluginHost • 0xad48d:$x1: NanoCore.ClientPluginHost • 0x47e8a:$x2: IClientNetworkHost • 0x7aaaa:$x2: IClientNetworkHost • 0xad4ca:$x2: IClientNetworkHost • 0x4b9bd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7e5dd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xb0ffd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.Quotation Details.exe.3aa95e8.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
11.2.Quotation Details.exe.3aa95e8.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0xf7c7:$s5: IClientLoggingHost
11.2.Quotation Details.exe.3aa95e8.2.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin
11.2.Quotation Details.exe.3aa95e8.2.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xf7ad:$a1: NanoCore.ClientPluginHost • 0xf778:$a2: NanoCore.ClientPlugin • 0xf7c7:$b9: IClientLoggingHost
1.2.Quotation Details.exe.41a2cc0.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 52 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242

Timestamp:	192.168.2.445.12.253.2424972658992816766 05/31/23-04:00:07.009857
SID:	2816766
Source Port:	49726
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242

Timestamp:	192.168.2.445.12.253.2424971658992816766 05/31/23-03:59:01.488743
SID:	2816766
Source Port:	49716
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242

Timestamp:	192.168.2.445.12.253.2424969258992816766 05/31/23-03:56:30.836452
SID:	2816766
Source Port:	49692
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242

Timestamp:	192.168.2.445.12.253.2424972158992025019 05/31/23-03:59:34.295435
SID:	2025019
Source Port:	49721
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970058992816766 05/31/23-03:57:08.650888
SID:	2816766
Source Port:	49700
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970658992816766 05/31/23-03:57:49.951823
SID:	2816766
Source Port:	49706
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971158992025019 05/31/23-03:58:24.970043
SID:	2025019
Source Port:	49711
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970158992025019 05/31/23-03:57:13.870857
SID:	2025019
Source Port:	49701
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971058992816766 05/31/23-03:58:19.657024
SID:	2816766
Source Port:	49710
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972758992025019 05/31/23-04:00:12.125417
SID:	2025019
Source Port:	49727
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971458992025019 05/31/23-03:58:45.735743
SID:	2025019
Source Port:	49714
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971758992025019 05/31/23-03:59:08.572866
SID:	2025019
Source Port:	49717

Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	−
Timestamp:	192.168.2.445.12.253.2424969858992816766 05/31/23-03:56:54.146303
SID:	2816766
Source Port:	49698
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	−
Timestamp:	192.168.2.445.12.253.2424970958992816718 05/31/23-03:58:12.396923
SID:	2816718
Source Port:	49709
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	−
Timestamp:	192.168.2.445.12.253.2424972458992025019 05/31/23-03:59:52.535511
SID:	2025019
Source Port:	49724
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	−
Timestamp:	192.168.2.445.12.253.2424972358992816766 05/31/23-03:59:47.414495
SID:	2816766
Source Port:	49723
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	−
Timestamp:	192.168.2.445.12.253.2424971358992816766 05/31/23-03:58:40.308766
SID:	2816766
Source Port:	49713
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	−
Timestamp:	192.168.2.445.12.253.2424970358992816766 05/31/23-03:57:29.347255
SID:	2816766
Source Port:	49703
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	−
Timestamp:	192.168.2.445.12.253.2424969958992816718 05/31/23-03:57:00.431618
SID:	2816718
Source Port:	49699
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970158992816766 05/31/23-03:57:14.834913
SID:	2816766
Source Port:	49701
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970858992816766 05/31/23-03:58:04.738849
SID:	2816766
Source Port:	49708
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971158992816766 05/31/23-03:58:26.204064
SID:	2816766
Source Port:	49711
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972658992025019 05/31/23-04:00:05.187162
SID:	2025019
Source Port:	49726
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971858992816766 05/31/23-03:59:17.099573
SID:	2816766
Source Port:	49718
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972158992816766 05/31/23-03:59:35.241904
SID:	2816766
Source Port:	49721
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971658992025019 05/31/23-03:58:59.883660
SID:	2025019
Source Port:	49716
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424969258992025019 05/31/23-03:56:25.759325
SID:	2025019
Source Port:	49692

Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424970758992025019 05/31/23-03:57:55.475825
SID:	2025019
Source Port:	49707
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424972058992816766 05/31/23-03:59:29.175573
SID:	2816766
Source Port:	49720
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424970258992816766 05/31/23-03:57:22.488525
SID:	2816766
Source Port:	49702
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424971958992816766 05/31/23-03:59:23.103459
SID:	2816766
Source Port:	49719
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424969358992025019 05/31/23-03:56:36.589109
SID:	2025019
Source Port:	49693
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424970658992025019 05/31/23-03:57:48.142985
SID:	2025019
Source Port:	49706
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424972558992025019 05/31/23-03:59:58.620724
SID:	2025019
Source Port:	49725
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.12.253.242 - Destination IP: 192.168.2.4	
Timestamp:	45.12.253.242192.168.2.45899496922841753 05/31/23-03:56:30.589443
SID:	2841753
Source Port:	5899
Destination Port:	49692
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970958992816766 05/31/23-03:58:12.396923
SID:	2816766
Source Port:	49709
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970858992025019 05/31/23-03:58:03.568164
SID:	2025019
Source Port:	49708
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424969458992025019 05/31/23-03:56:47.050579
SID:	2025019
Source Port:	49694
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971858992025019 05/31/23-03:59:15.425860
SID:	2025019
Source Port:	49718
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424969958992816766 05/31/23-03:57:01.461077
SID:	2816766
Source Port:	49699
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971558992025019 05/31/23-03:58:52.346146
SID:	2025019
Source Port:	49715
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970558992025019 05/31/23-03:57:40.488645
SID:	2025019
Source Port:	49705

Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971258992816766 05/31/23-03:58:34.052236
SID:	2816766
Source Port:	49712
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970758992816766 05/31/23-03:57:57.856787
SID:	2816766
Source Port:	49707
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.12.253.242 - Destination IP: 192.168.2.4	
Timestamp:	45.12.253.242192.168.2.45899497132810290 05/31/23-03:58:40.151665
SID:	2810290
Source Port:	5899
Destination Port:	49713
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971758992816766 05/31/23-03:59:10.025241
SID:	2816766
Source Port:	49717
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972058992025019 05/31/23-03:59:28.244511
SID:	2025019
Source Port:	49720
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972258992816766 05/31/23-03:59:41.289827
SID:	2816766
Source Port:	49722
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972758992816766 05/31/23-04:00:13.057662
SID:	2816766
Source Port:	49727
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424969458992816766 05/31/23-03:56:48.090304
SID:	2816766
Source Port:	49694
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970058992025019 05/31/23-03:57:07.149878
SID:	2025019
Source Port:	49700
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971058992025019 05/31/23-03:58:18.373829
SID:	2025019
Source Port:	49710
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971858992816718 05/31/23-03:59:16.099293
SID:	2816718
Source Port:	49718
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970358992025019 05/31/23-03:57:27.579932
SID:	2025019
Source Port:	49703
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971358992025019 05/31/23-03:58:39.081495
SID:	2025019
Source Port:	49713
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424969958992025019 05/31/23-03:56:59.566501
SID:	2025019
Source Port:	49699
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.12.253.242 - Destination IP: 192.168.2.4	
Timestamp:	45.12.253.242192.168.2.45899496942810290 05/31/23-03:56:47.496805
SID:	2810290
Source Port:	5899

Destination Port:	49694
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424972358992025019 05/31/23-03:59:46.392270
SID:	2025019
Source Port:	49723
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424972458992816766 05/31/23-03:59:53.493126
SID:	2816766
Source Port:	49724
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424970458992816766 05/31/23-03:57:35.533816
SID:	2816766
Source Port:	49704
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424969858992025019 05/31/23-03:56:53.190117
SID:	2025019
Source Port:	49698
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424970958992025019 05/31/23-03:58:11.627033
SID:	2025019
Source Port:	49709
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424971258992025019 05/31/23-03:58:31.969396
SID:	2025019
Source Port:	49712
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	▬
Timestamp:	192.168.2.445.12.253.2424971958992025019 05/31/23-03:59:22.203113
SID:	2025019
Source Port:	49719
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972258992025019 05/31/23-03:59:40.358095
SID:	2025019
Source Port:	49722
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424972558992816766 05/31/23-03:59:59.543859
SID:	2816766
Source Port:	49725
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424969358992816766 05/31/23-03:56:38.356653
SID:	2816766
Source Port:	49693
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424971558992816766 05/31/23-03:58:53.787555
SID:	2816766
Source Port:	49715
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970258992025019 05/31/23-03:57:20.083306
SID:	2025019
Source Port:	49702
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 45.12.253.242	
Timestamp:	192.168.2.445.12.253.2424970558992816766 05/31/23-03:57:41.435019
SID:	2816766
Source Port:	49705
Destination Port:	5899
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

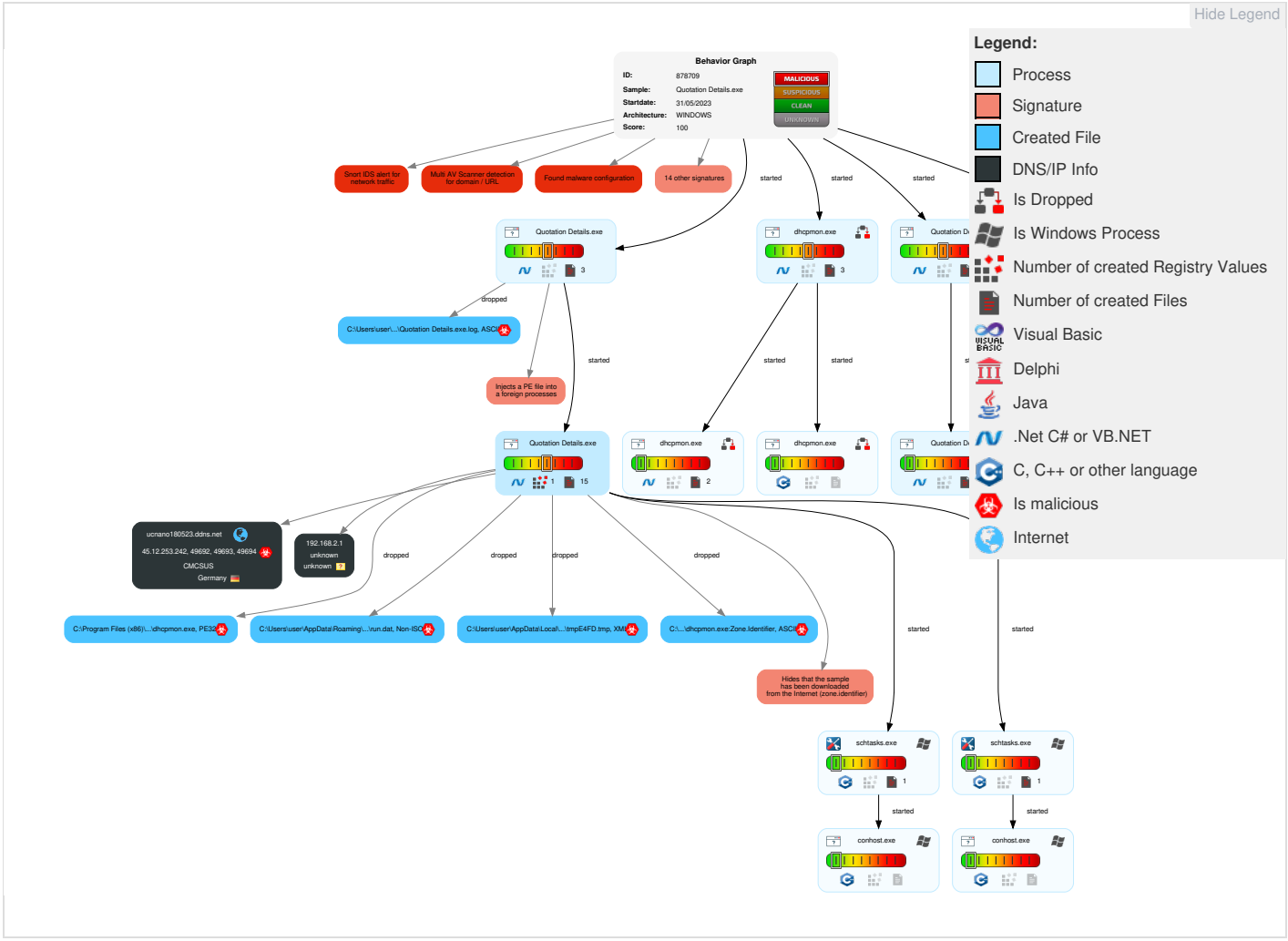
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	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	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 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)	Logon Script (Windows)	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 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 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

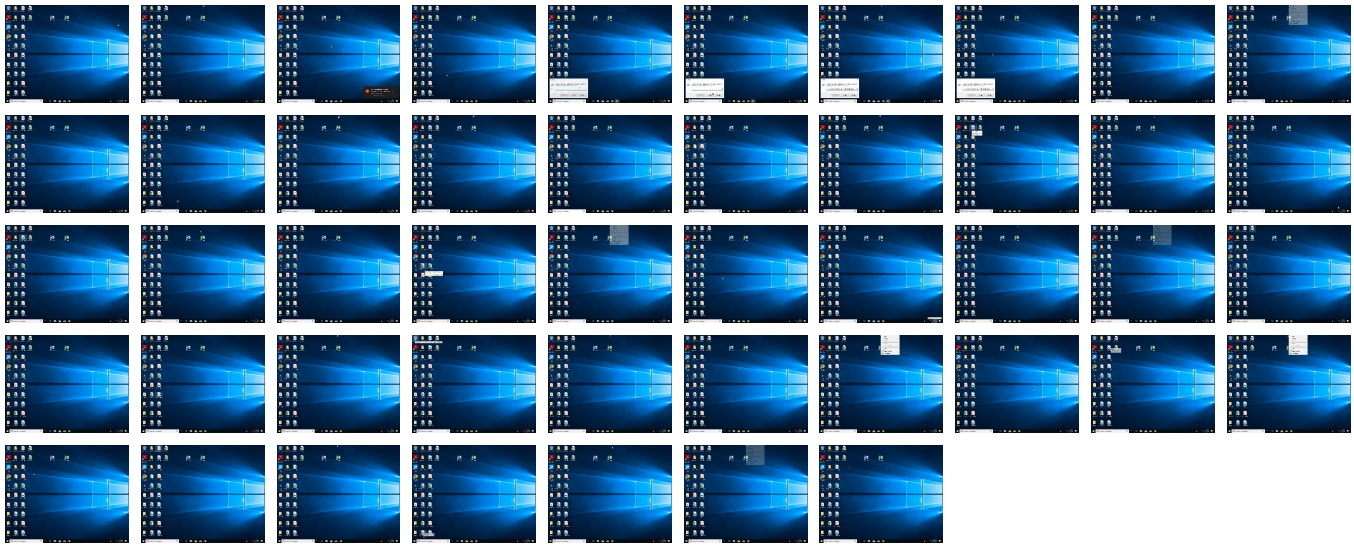
Behavior Graph



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
Quotation Details.exe	42%	ReversingLabs	Win32.Trojan.Pwsx	
Quotation Details.exe	55%	Virustotal		Browse
Quotation Details.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	42%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ucnano180523.ddns.net	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.founder.com.cn/cnIT	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnIT	1%	Virustotal		Browse
http://www.founder.com.cn/cns	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ZvM	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/6va	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/iv	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/Ev4	0%	Avira URL Cloud	safe	
http://www.fontbureau.comionawv&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/)v	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/6va	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.html	0%	Avira URL Cloud	safe	
ucnano180523.ddns.net	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcy	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/wv&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Ev4	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ucnano180523.ddns.net	45.12.253.242	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ucnano180523.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnIT	Quotation Details.exe, 00000001.00000003.545506291.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ZvM	Quotation Details.exe, 00000001.00000003.548388819.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548217840.0000000005EDA000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548453978.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548068960.0000000005EDA000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548554025.0000000005ED8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/6va	Quotation Details.exe, 00000001.00000003.547570175.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.547404517.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

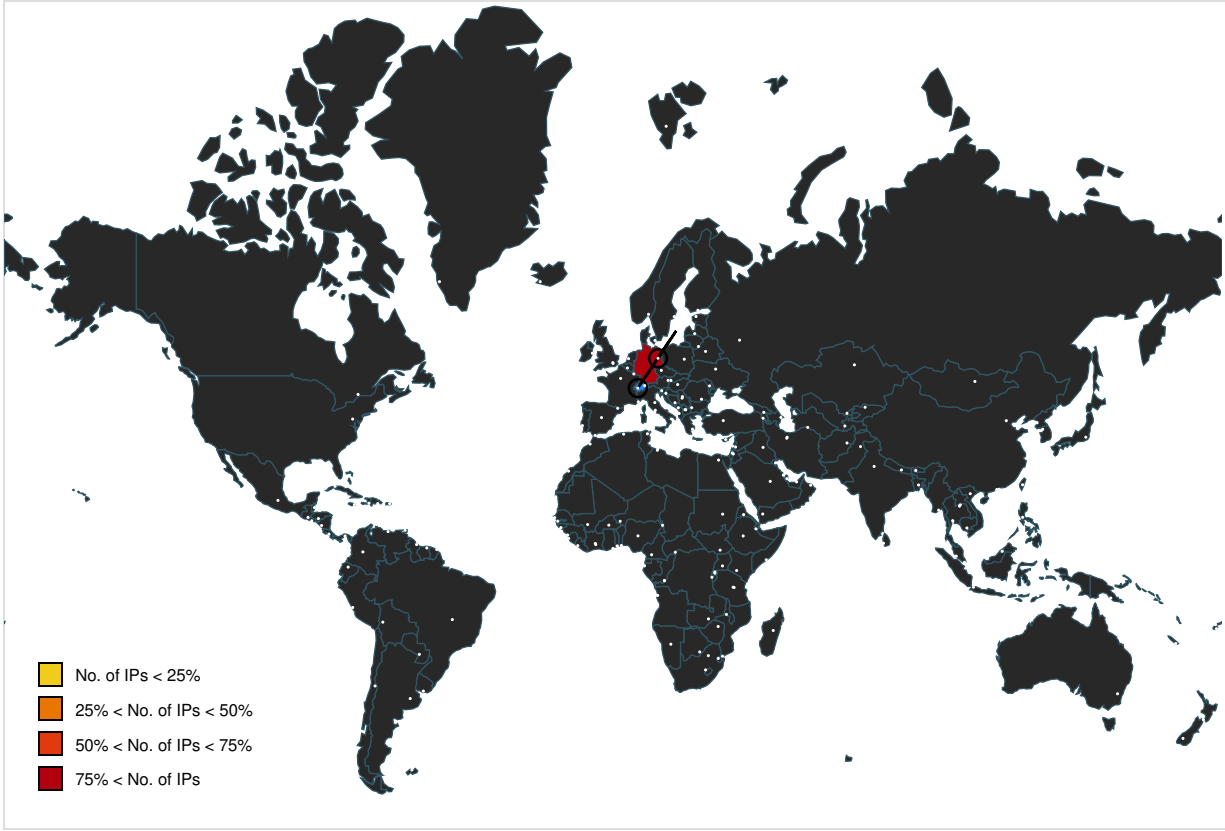
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Quotation Details.exe, 00000001.00000003 .545081296.0000000005EEB000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.543997545 .0000000005EEB000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000002.568320134.0000000007032000.00 000004.00000800.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .544102018.0000000005EEB000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.544324148 .0000000005EEB000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.543851711.0000000005EEB000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .544923288.0000000005EEB000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.544135306 .0000000005EEB000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.544576997.0000000005EEB000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .545124936.0000000005EEB000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.544981372 .0000000005EEB000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.544453838.0000000005EEB000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .544885298.0000000005EEB000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.544065041 .0000000005EEB000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.544853168.0000000005EEB000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .544647907.0000000005EEB000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.544265316 .0000000005EEB000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.543937043.0000000005EEB000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .544537246.0000000005EEB000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.543970292 .0000000005EEB000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.544010760.0000000005EEB000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Quotation Details.exe, 00000001.00000002 .568320134.0000000007032000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Quotation Details.exe, 00000001.00000002 .568320134.0000000007032000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Quotation Details.exe, 00000001.00000002 .568320134.0000000007032000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Quotation Details.exe, 00000001.00000002 .568320134.0000000007032000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)v	Quotation Details.exe, 00000001.00000003 .548388819.0000000005ED2000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548217840 .0000000005EDA000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.548453978.0000000005ED2000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .548068960.0000000005EDA000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548554025 .0000000005ED8000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cns	Quotation Details.exe, 00000001.00000003 .545546949.0000000005F0D000.00000004.000 00020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Quotation Details.exe, 00000001.00000003.548554025.0000000005ED8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.html	Quotation Details.exe, 00000001.00000003.553838850.0000000005EDC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/Ev4	Quotation Details.exe, 00000001.00000003.548388819.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548453978.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548554025.0000000005ED8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548959861.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.549053710.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.549004017.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.549031471.0000000005F16000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnd	Quotation Details.exe, 00000001.00000003.545506291.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comcy	Quotation Details.exe, 00000001.00000003.548377237.0000000005EDC000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548541678.0000000005EDC000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548420477.0000000005EDE000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548217840.0000000005EDE000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.547570175.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.547404517.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548068960.0000000005EDA000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548329912.0000000005EDC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.562763120.0000000005ED0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	Quotation Details.exe, 00000001.00000003.554105421.0000000005ED8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/P	Quotation Details.exe, 00000001.00000003 .548388819.0000000005ED2000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548217840 .0000000005EDA000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.548453978.0000000005ED2000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .547570175.0000000005ED2000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.547404517 .0000000005ED2000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.548068960.0000000005EDA000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .548554025.0000000005ED8000.00000004.000 00020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comionawv&	Quotation Details.exe, 00000001.00000003 .562763120.0000000005ED0000.00000004.000 00020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/6va	Quotation Details.exe, 00000001.00000003 .548388819.0000000005ED2000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548217840 .0000000005EDA000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.548453978.0000000005ED2000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .548068960.0000000005EDA000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548554025 .0000000005ED8000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Quotation Details.exe, 00000001.00000003 .548388819.0000000005ED2000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548217840 .0000000005EDA000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.548453978.0000000005ED2000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .548068960.0000000005EDA000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548554025 .0000000005ED8000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/wv&	Quotation Details.exe, 00000001.00000003 .548554025.0000000005ED8000.00000004.000 00020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Quotation Details.exe, 00000001.00000002 .568320134.0000000007032000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Quotation Details.exe, 00000001.00000002 .568320134.0000000007032000.00000004.000 00800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Quotation Details.exe, 00000001.00000003 .545601428.0000000005F0D000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.545546949 .0000000005F0D000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	Quotation Details.exe, 00000001.00000003 .548388819.0000000005ED2000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548217840 .0000000005EDA000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.548453978.0000000005ED2000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .547570175.0000000005ED2000.00000004.000 00020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.547404517 .0000000005ED2000.00000004.00000020.0002 0000.00000000.sdmp, Quotation Details.exe, 0000000 1.00000003.548068960.0000000005EDA000.00 000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003 .548554025.0000000005ED8000.00000004.000 00020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/	Quotation Details.exe, 00000001.00000003.548388819.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548453978.0000000005ED2000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548554025.0000000005ED8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.	Quotation Details.exe, 00000001.00000003.554999096.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.554980127.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.555039584.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.555016211.0000000005F16000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designP	Quotation Details.exe, 00000001.00000003.550525064.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550699168.0000000005F17000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550558059.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550467557.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550499127.0000000005F17000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550644679.0000000005F17000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550597180.0000000005F17000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.comt	Quotation Details.exe, 00000001.00000003.562763120.0000000005ED0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/iv	Quotation Details.exe, 00000001.00000003.548554025.0000000005ED8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Quotation Details.exe, 00000001.00000003.548554025.0000000005ED8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Quotation Details.exe, 00000001.00000002.568320134.0000000007032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/	Quotation Details.exe, 00000001.00000003.550212944.0000000005F17000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550286641.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550396489.0000000005F17000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550324044.0000000005F17000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550429788.0000000005F17000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550245065.0000000005F16000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.550355346.0000000005F17000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Ev4	Quotation Details.exe, 00000001.00000003.548217840.0000000005EDA000.00000004.00000020.00020000.00000000.sdmp, Quotation Details.exe, 00000001.00000003.548068960.0000000005EDA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.12.253.242	ucnano180523.ddns.net	Germany		33657	CMCSUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878709
Start date and time:	2023-05-31 03:55:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Quotation Details.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@22/11@33/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

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

Simulations

Behavior and APIs

Time	Type	Description
03:56:17	API Interceptor	1954x Sleep call for process: Quotation Details.exe modified
03:56:23	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Quotation Details.exe" s>$(Arg0)
03:56:24	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
03:56:25	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
03:56:30	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Quotation Details.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	782336
Entropy (8bit):	7.67780755150778
Encrypted:	false
SSDEEP:	12288:MRP2B0xTGlxNqvNu2hZ+nUEsn9lu8fFUjXHvMeP/ppubvhRwL7kBfZkOcZRGUdyH:IPLaVUH9993FUFHib7wLKbcZRisY
MD5:	5EC7A9D9A56FA3EB2D6F63A555969A37
SHA1:	77719C19C79E9A1FF120981A78BF8DDA6BE321C5
SHA-256:	DEE80FF02E834FAC0E59395BB2AD3A39698208DBF02EED0E7697F6D2A9D604DB
SHA-512:	8ACF485DD2B8B66B28133DDC68233D0AE9DF71978F3A690F0C754BEBB003E2BEE87E60E7D7EE9A124AB481E1B2F6191E9D282E8A51BCCCFB6FCBED2225859C63
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Hud.....0.....P..... .....@.. ....@.....O.....<:.....`...T..... ..... ..H.....text..... ..... ..`.rsrc...<:.....@.....@..@.relo c.....@..B..... ....

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

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

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

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

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859

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

C:\Users\user\AppData\Local\Temp\tmpE4FD.tmp

Process:	C:\Users\user\Desktop\Quotation Details.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1307
Entropy (8bit):	5.090550108749449
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Ys63xtn:cbk4oL600QydbQxIYODOLedq34Ej
MD5:	91DCDC886A0EFF0DA2FA8ECF8DEB1E97
SHA1:	8B07D57AFACF67072F811CA197957C4239969306
SHA-256:	7FD14E9B979ACAF5A9276B80C021AEB4F54C136F5A12EED6250E590236311F19
SHA-512:	F18B66EA75FC4C2FCFD0F6BDBA9E3F661A492D7FC699F3803F34AF123C2A60209403BE05578B93AB48428584635FBFE6FDC126A6C4CEDAEB2C158769DA13A673
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\tmpE6C3.tmp

Process:	C:\Users\user\Desktop\Quotation Details.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\Quotation Details.exe
File Type:	data
Category:	dropped
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\Quotation Details.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:Ton:0n
MD5:	FFC60B4CCB85F50FF3C0055520E2FF90
SHA1:	49D2630B3926D64D3435FFB4B689846A4299C98C
SHA-256:	98150A036795F6449CD03BEFF707CEAAA2DCEDE425990B417766A67301D97CE1
SHA-512:	0D6E6AB79B1A8854A7EAF3ADF316BFEAC1C36594733F515AF5ACA7E124B1908AC425C9B2C5839B60DCCD2ADFB331DA694FF05CA6992195B3D860F4ED62FE1568
Malicious:	**true**
Preview:	..;za.H

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

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

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

Process:	C:\Users\user\Desktop\Quotation Details.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5CCA
Malicious:	false

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

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

Process:	C:\Users\user\Desktop\Quotation Details.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.115808539574485
Encrypted:	false
SSDEEP:	3:oNt+WfW0fyMQh94A:oNwv0fyz+A
MD5:	D2671C11D14B859D0436289526D51188
SHA1:	CCA894322508B19C74F73BB3AE96E62B83C2E314
SHA-256:	6162C7AEC17B46C5910F4417F9E2A3B3FD8FFDCE187CFBEE1037A5134612E000
SHA-512:	7B77B4940F37E9584C3013F1FC3405D85A9720555EA52D3C9924867EA50331BAF96AADA1D4A5261E7DDF3594BC0532253BA3C381BD710C908E84A6571EE12235
Malicious:	false
Preview:	C:\Users\user\Desktop\Quotation Details.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.67780755150778
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Quotation Details.exe
File size:	782336
MD5:	5ec7a9d9a56fa3eb2d6f63a555969a37
SHA1:	77719c19c79e9a1ff120981a78bf8dda6be321c5
SHA256:	dee80ff02e834fac0e59395bb2ad3a39698208dbf02eed0e7697f6d2a9d604db
SHA512:	8acf485dd2b8b66b28133ddc68233d0ae9df71978f3a690f0c754bebb003e2bee87e60e7d7ee9a124ab481e1b2f6191e9d282e8a51bcccfb6fcbed2225859c63
SSDEEP:	12288:MRP2B0xTGlxNqvNu2hZ+nUEsn9lu8fFUjXHvMeP/ppubvhRwL7kBfZkOcZRGUdyH:IPLaVUH9993FUFHib7wLKbcZRisY
TLSH:	3CF42254665B846FC2C72FF40C8463B1A2EC83CABD7AEB271C12B4E4DA47F4A144579A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Hud.....0.....P..... .....@.. ....@.....

File Icon

Icon Hash:	94969edbd9f8d9c6

Static PE Info

General

Entrypoint:	0x4babea
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x647548EE [Tue May 30 00:53:02 2023 UTC]
TLS Callbacks:	

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

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbab96	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x3a3c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb9b60	0x54	.text

Name	Virtual Address	Virtual Size	Is in Section
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	0xb8bf0	0xb9000	False	0.9320497255067568	data	7.7081753259071135	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x3a3c	0x4000	False	0.8494873046875	data	7.3967994906792525	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x1000	False	0.0087890625	data	0.016408464515625623	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbc0c8	0x36fd	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xbf7d8	0x14	data		
RT_VERSION	0xbf7fc	0x23c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.445.12.253.2424972658992816766 05/31/23-04:00:07.009857	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49726	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971658992816766 05/31/23-03:59:01.488743	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424969258992816766 05/31/23-03:56:30.836452	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49692	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972158992025019 05/31/23-03:59:34.295435	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970058992816766 05/31/23-03:57:08.650888	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49700	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970658992816766 05/31/23-03:57:49.951823	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	5899	192.168.2.4	45.12.253.242

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.445.12.253.2424971158992025019 05/31/23-03:58:24.970043	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970158992025019 05/31/23-03:57:13.870857	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971058992816766 05/31/23-03:58:19.657024	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972758992025019 05/31/23-04:00:12.125417	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971458992025019 05/31/23-03:58:45.735743	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971758992025019 05/31/23-03:59:08.572866	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424969858992816766 05/31/23-03:56:54.146303	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49698	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970958992816718 05/31/23-03:58:12.396923	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49709	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972458992025019 05/31/23-03:59:52.535511	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972358992816766 05/31/23-03:59:47.414495	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971358992816766 05/31/23-03:58:40.308766	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970358992816766 05/31/23-03:57:29.347255	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424969958992816718 05/31/23-03:57:00.431618	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49699	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970158992816766 05/31/23-03:57:14.834913	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970858992816766 05/31/23-03:58:04.738849	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971158992816766 05/31/23-03:58:26.204064	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972658992025019 05/31/23-04:00:05.187162	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971858992816766 05/31/23-03:59:17.099573	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972158992816766 05/31/23-03:59:35.241904	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49721	5899	192.168.2.4	45.12.253.242

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.445.12.253.242 4971658992025019 05/31/23-03:58:59.883660	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4969258992025019 05/31/23-03:56:25.759325	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49692	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4970758992025019 05/31/23-03:57:55.475825	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4972058992816766 05/31/23-03:59:29.175573	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4970258992816766 05/31/23-03:57:22.488525	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4971958992816766 05/31/23-03:59:23.103459	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4969358992025019 05/31/23-03:56:36.589109	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49693	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4970658992025019 05/31/23-03:57:48.142985	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4972558992025019 05/31/23-03:59:58.620724	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	5899	192.168.2.4	45.12.253.242
45.12.253.242192.168.2.4 5899496922841753 05/31/23-03:56:30.589443	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	5899	49692	45.12.253.242	192.168.2.4
192.168.2.445.12.253.242 4970958992816766 05/31/23-03:58:12.396923	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4970858992025019 05/31/23-03:58:03.568164	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4969458992025019 05/31/23-03:56:47.050579	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49694	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4971858992025019 05/31/23-03:59:15.425860	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4969958992816766 05/31/23-03:57:01.461077	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49699	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4971558992025019 05/31/23-03:58:52.346146	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4970558992025019 05/31/23-03:57:40.488645	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4971258992816766 05/31/23-03:58:34.052236	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.242 4970758992816766 05/31/23-03:57:57.856787	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	5899	192.168.2.4	45.12.253.242

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.12.253.242192.168.2.45899497132810290 05/31/23-03:58:40.151665	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5899	49713	45.12.253.242	192.168.2.4
192.168.2.445.12.253.2424971758992816766 05/31/23-03:59:10.025241	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972058992025019 05/31/23-03:59:28.244511	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972258992816766 05/31/23-03:59:41.289827	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972758992816766 05/31/23-04:00:13.057662	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49727	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424969458992816766 05/31/23-03:56:48.090304	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49694	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970058992025019 05/31/23-03:57:07.149878	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971058992025019 05/31/23-03:58:18.373829	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971858992816718 05/31/23-03:59:16.099293	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49718	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970358992025019 05/31/23-03:57:27.579932	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971358992025019 05/31/23-03:58:39.081495	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424969958992025019 05/31/23-03:56:59.566501	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	5899	192.168.2.4	45.12.253.242
45.12.253.242192.168.2.45899496942810290 05/31/23-03:56:47.496805	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5899	49694	45.12.253.242	192.168.2.4
192.168.2.445.12.253.2424972358992025019 05/31/23-03:59:46.392270	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972458992816766 05/31/23-03:59:53.493126	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49724	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970458992816766 05/31/23-03:57:35.533816	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424969858992025019 05/31/23-03:56:53.190117	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970958992025019 05/31/23-03:58:11.627033	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971258992025019 05/31/23-03:58:31.969396	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	5899	192.168.2.4	45.12.253.242

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.445.12.253.2424971958992025019 05/31/23-03:59:22.203113	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972258992025019 05/31/23-03:59:40.358095	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424972558992816766 05/31/23-03:59:59.543859	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49725	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424969358992816766 05/31/23-03:56:38.356653	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49693	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424971558992816766 05/31/23-03:58:53.787555	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970258992025019 05/31/23-03:57:20.083306	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	5899	192.168.2.4	45.12.253.242
192.168.2.445.12.253.2424970558992816766 05/31/23-03:57:41.435019	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	5899	192.168.2.4	45.12.253.242

Network Port Distribution

Total Packets: 69

- 53 (DNS)
- 5899 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 03:56:25.531831980 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:25.560472965 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:25.560745001 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:25.759325027 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:25.838757038 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:25.838912964 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:25.883755922 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.011210918 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.223103046 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.250231028 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.276443958 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.354517937 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.444910049 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.444981098 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.445035934 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.445092916 CEST	5899	49692	45.12.253.242	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 03:56:26.445142031 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.445199966 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.471662998 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.471735001 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.471791983 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.471833944 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.471863985 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.471924067 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.471946955 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.471978903 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.472033024 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.472038031 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.472088099 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.472143888 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498102903 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498168945 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498224974 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498289108 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498296022 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498356104 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498361111 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498413086 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498467922 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498492002 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498522997 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498579025 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498588085 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498631954 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498687029 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498688936 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498744965 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498797894 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498801947 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498857021 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498912096 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.498912096 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.498980999 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.499037027 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.525347948 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525438070 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525497913 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525554895 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525554895 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.525614023 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525646925 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.525671959 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525728941 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525734901 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.525787115 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525837898 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.525841951 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525897980 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.525949955 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.525954962 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526015043 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526072025 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526073933 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526128054 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526184082 CEST	5899	49692	45.12.253.242	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 03:56:26.526185989 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526246071 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526299000 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526303053 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526360035 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526411057 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526416063 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526472092 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526527882 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526530027 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526585102 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526635885 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526640892 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526698112 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526753902 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526772022 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526812077 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526870012 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526880980 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526937962 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.526988029 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.526992083 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.527046919 CEST	5899	49692	45.12.253.242	192.168.2.4
May 31, 2023 03:56:26.527095079 CEST	49692	5899	192.168.2.4	45.12.253.242
May 31, 2023 03:56:26.527101040 CEST	5899	49692	45.12.253.242	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 03:56:25.428962946 CEST	59683	53	192.168.2.4	8.8.8.8
May 31, 2023 03:56:25.465596914 CEST	53	59683	8.8.8.8	192.168.2.4
May 31, 2023 03:56:36.539118052 CEST	64167	53	192.168.2.4	8.8.8.8
May 31, 2023 03:56:36.560214043 CEST	53	64167	8.8.8.8	192.168.2.4
May 31, 2023 03:56:46.999397993 CEST	58565	53	192.168.2.4	8.8.8.8
May 31, 2023 03:56:47.020541906 CEST	53	58565	8.8.8.8	192.168.2.4
May 31, 2023 03:56:53.121328115 CEST	60686	53	192.168.2.4	8.8.8.8
May 31, 2023 03:56:53.159699917 CEST	53	60686	8.8.8.8	192.168.2.4
May 31, 2023 03:56:59.515897989 CEST	61124	53	192.168.2.4	8.8.8.8
May 31, 2023 03:56:59.536422968 CEST	53	61124	8.8.8.8	192.168.2.4
May 31, 2023 03:57:06.878510952 CEST	59444	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:06.898711920 CEST	53	59444	8.8.8.8	192.168.2.4
May 31, 2023 03:57:13.813244104 CEST	55570	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:13.840467930 CEST	53	55570	8.8.8.8	192.168.2.4
May 31, 2023 03:57:20.025006056 CEST	64906	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:20.053575039 CEST	53	64906	8.8.8.8	192.168.2.4
May 31, 2023 03:57:27.530657053 CEST	59446	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:27.551162958 CEST	53	59446	8.8.8.8	192.168.2.4
May 31, 2023 03:57:35.186477900 CEST	50861	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:35.214668036 CEST	53	50861	8.8.8.8	192.168.2.4
May 31, 2023 03:57:40.406709909 CEST	61088	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:40.432471991 CEST	53	61088	8.8.8.8	192.168.2.4
May 31, 2023 03:57:47.809973001 CEST	58729	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:47.836530924 CEST	53	58729	8.8.8.8	192.168.2.4
May 31, 2023 03:57:55.374121904 CEST	64700	53	192.168.2.4	8.8.8.8
May 31, 2023 03:57:55.442423105 CEST	53	64700	8.8.8.8	192.168.2.4
May 31, 2023 03:58:03.514790058 CEST	56022	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:03.536453962 CEST	53	56022	8.8.8.8	192.168.2.4
May 31, 2023 03:58:11.356097937 CEST	60822	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:11.376375914 CEST	53	60822	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 03:58:18.318727970 CEST	49750	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:18.345449924 CEST	53	49750	8.8.8.8	192.168.2.4
May 31, 2023 03:58:24.905312061 CEST	60550	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:24.934217930 CEST	53	60550	8.8.8.8	192.168.2.4
May 31, 2023 03:58:31.910937071 CEST	54851	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:31.938338041 CEST	53	54851	8.8.8.8	192.168.2.4
May 31, 2023 03:58:39.020291090 CEST	57300	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:39.052367926 CEST	53	57300	8.8.8.8	192.168.2.4
May 31, 2023 03:58:45.686958075 CEST	54521	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:45.707653046 CEST	53	54521	8.8.8.8	192.168.2.4
May 31, 2023 03:58:51.902966976 CEST	58914	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:51.944811106 CEST	53	58914	8.8.8.8	192.168.2.4
May 31, 2023 03:58:59.820317984 CEST	51419	53	192.168.2.4	8.8.8.8
May 31, 2023 03:58:59.849915981 CEST	53	51419	8.8.8.8	192.168.2.4
May 31, 2023 03:59:07.705219030 CEST	51054	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:07.726438046 CEST	53	51054	8.8.8.8	192.168.2.4
May 31, 2023 03:59:15.351322889 CEST	55673	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:15.395586014 CEST	53	55673	8.8.8.8	192.168.2.4
May 31, 2023 03:59:22.133614063 CEST	49735	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:22.156400919 CEST	53	49735	8.8.8.8	192.168.2.4
May 31, 2023 03:59:28.191653967 CEST	52437	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:28.214536905 CEST	53	52437	8.8.8.8	192.168.2.4
May 31, 2023 03:59:34.228857040 CEST	52825	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:34.264384985 CEST	53	52825	8.8.8.8	192.168.2.4
May 31, 2023 03:59:40.298445940 CEST	58530	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:40.327013969 CEST	53	58530	8.8.8.8	192.168.2.4
May 31, 2023 03:59:46.319281101 CEST	64959	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:46.345963001 CEST	53	64959	8.8.8.8	192.168.2.4
May 31, 2023 03:59:52.477865934 CEST	63093	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:52.506506920 CEST	53	63093	8.8.8.8	192.168.2.4
May 31, 2023 03:59:58.553975105 CEST	50433	53	192.168.2.4	8.8.8.8
May 31, 2023 03:59:58.588646889 CEST	53	50433	8.8.8.8	192.168.2.4
May 31, 2023 04:00:04.980314970 CEST	53498	53	192.168.2.4	8.8.8.8
May 31, 2023 04:00:05.002305031 CEST	53	53498	8.8.8.8	192.168.2.4
May 31, 2023 04:00:12.072873116 CEST	61460	53	192.168.2.4	8.8.8.8
May 31, 2023 04:00:12.096570969 CEST	53	61460	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 03:56:25.428962946 CEST	192.168.2.4	8.8.8.8	0xcaa6	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:36.539118052 CEST	192.168.2.4	8.8.8.8	0x9872	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:46.999397993 CEST	192.168.2.4	8.8.8.8	0x1a22	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:53.121328115 CEST	192.168.2.4	8.8.8.8	0x9249	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:59.515897989 CEST	192.168.2.4	8.8.8.8	0x16ea	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:06.878510952 CEST	192.168.2.4	8.8.8.8	0x90db	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:13.813244104 CEST	192.168.2.4	8.8.8.8	0xbcdb	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:20.025006056 CEST	192.168.2.4	8.8.8.8	0x85d	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:27.530657053 CEST	192.168.2.4	8.8.8.8	0x5d1b	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:35.186477900 CEST	192.168.2.4	8.8.8.8	0x9329	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:40.406709909 CEST	192.168.2.4	8.8.8.8	0xf9ba	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 03:57:47.809973001 CEST	192.168.2.4	8.8.8.8	0xe469	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:55.374121904 CEST	192.168.2.4	8.8.8.8	0x61f1	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:03.514790058 CEST	192.168.2.4	8.8.8.8	0x2002	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:11.356097937 CEST	192.168.2.4	8.8.8.8	0x1e	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:18.318727970 CEST	192.168.2.4	8.8.8.8	0x7bd4	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:24.905312061 CEST	192.168.2.4	8.8.8.8	0xfa18	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:31.910937071 CEST	192.168.2.4	8.8.8.8	0x543f	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:39.020291090 CEST	192.168.2.4	8.8.8.8	0x1fa9	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:45.686958075 CEST	192.168.2.4	8.8.8.8	0x2fa2	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:51.902966976 CEST	192.168.2.4	8.8.8.8	0xdcdf	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:59.820317984 CEST	192.168.2.4	8.8.8.8	0x1d84	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:07.705219030 CEST	192.168.2.4	8.8.8.8	0xc269	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:15.351322889 CEST	192.168.2.4	8.8.8.8	0x9313	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:22.133614063 CEST	192.168.2.4	8.8.8.8	0x225a	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:28.191653967 CEST	192.168.2.4	8.8.8.8	0x891c	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:34.228857040 CEST	192.168.2.4	8.8.8.8	0xdd62	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:40.298445940 CEST	192.168.2.4	8.8.8.8	0xab23	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:46.319281101 CEST	192.168.2.4	8.8.8.8	0x80d7	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:52.477865934 CEST	192.168.2.4	8.8.8.8	0x1261	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:58.553975105 CEST	192.168.2.4	8.8.8.8	0xf13a	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 04:00:04.980314970 CEST	192.168.2.4	8.8.8.8	0x5330	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false
May 31, 2023 04:00:12.072873116 CEST	192.168.2.4	8.8.8.8	0x3b0a	Standard query (0)	ucnano180523.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

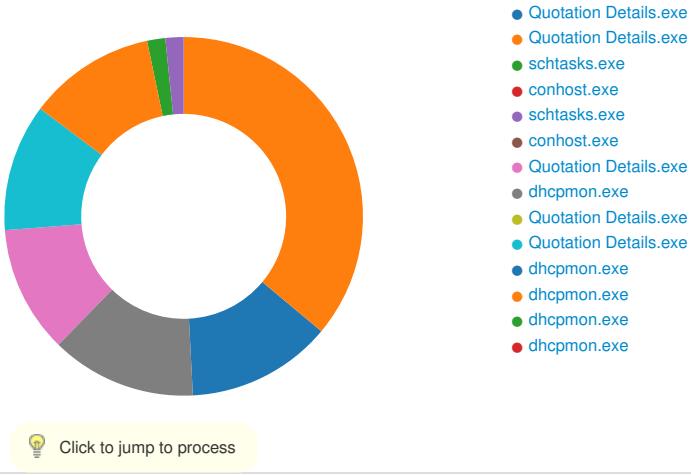
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 03:56:25.465596914 CEST	8.8.8.8	192.168.2.4	0xcaa6	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:36.560214043 CEST	8.8.8.8	192.168.2.4	0x9872	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:47.020541906 CEST	8.8.8.8	192.168.2.4	0x1a22	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:53.159699917 CEST	8.8.8.8	192.168.2.4	0x9249	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:56:59.536422968 CEST	8.8.8.8	192.168.2.4	0x16ea	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:06.898711920 CEST	8.8.8.8	192.168.2.4	0x90db	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:13.840467930 CEST	8.8.8.8	192.168.2.4	0xbcdb	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 03:57:20.053575039 CEST	8.8.8.8	192.168.2.4	0x85d	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:27.551162958 CEST	8.8.8.8	192.168.2.4	0x5d1b	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:35.214668036 CEST	8.8.8.8	192.168.2.4	0x9329	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:40.432471991 CEST	8.8.8.8	192.168.2.4	0xf9ba	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:47.836530924 CEST	8.8.8.8	192.168.2.4	0xe469	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:57:55.442423105 CEST	8.8.8.8	192.168.2.4	0x61f1	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:03.536453962 CEST	8.8.8.8	192.168.2.4	0x2002	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:11.376375914 CEST	8.8.8.8	192.168.2.4	0x1e	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:18.345449924 CEST	8.8.8.8	192.168.2.4	0x7bd4	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:24.934217930 CEST	8.8.8.8	192.168.2.4	0xfa18	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:31.938338041 CEST	8.8.8.8	192.168.2.4	0x543f	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:39.052367926 CEST	8.8.8.8	192.168.2.4	0x1fa9	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:45.707653046 CEST	8.8.8.8	192.168.2.4	0x2fa2	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:51.944811106 CEST	8.8.8.8	192.168.2.4	0xdcdf	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:58:59.849915981 CEST	8.8.8.8	192.168.2.4	0x1d84	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:07.726438046 CEST	8.8.8.8	192.168.2.4	0xc269	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:15.395586014 CEST	8.8.8.8	192.168.2.4	0x9313	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:22.156400919 CEST	8.8.8.8	192.168.2.4	0x225a	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:28.214536905 CEST	8.8.8.8	192.168.2.4	0x891c	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:34.264384985 CEST	8.8.8.8	192.168.2.4	0xdd62	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:40.327013969 CEST	8.8.8.8	192.168.2.4	0xab23	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:46.345963001 CEST	8.8.8.8	192.168.2.4	0x80d7	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:52.506506920 CEST	8.8.8.8	192.168.2.4	0x1261	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 03:59:58.588646889 CEST	8.8.8.8	192.168.2.4	0xf13a	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false
May 31, 2023 04:00:05.002305031 CEST	8.8.8.8	192.168.2.4	0x5330	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 04:00:12.096570969 CEST	8.8.8.8	192.168.2.4	0x3b0a	No error (0)	ucnano180523.ddns.net		45.12.253.242	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: Quotation Details.exe PID: 7120, Parent PID: 3528

General

Target ID:	1
Start time:	03:56:10
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\Quotation Details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation Details.exe
Imagebase:	0xc40000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.565244380.000000000416B000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.565244380.000000000416B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.565244380.000000000416B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.565244380.000000000416B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation Details.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation Details.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7312C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: Quotation Details.exe PID: **5328**, Parent PID: **7120**

General

Target ID:	3
Start time:	03:56:20
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\Quotation Details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation Details.exe
Imagebase:	0xf50000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000003.578596362.0000000001511000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	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	71C6BEFF	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	71C61E60	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	71C6BEFF	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	71C6DD66	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	71C6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE4FD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71C67038	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	71C61E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE6C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71C67038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	71C6BEFF	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	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	27	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE4FD.tmp	success or wait	1	71C66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE6C3.tmp	success or wait	1	71C66A95	DeleteFileW
C:\Users\user\Desktop\Quotation Details.exe:Zone.Identifier	success or wait	1	71BE2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	cd fd 3b 7a 61 fd 48	;zaH	success or wait	1	71C61B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 48 75 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0b 00 00 50 00 00 00 00 00 00 fd 0b 00 00 20 00 00 00 fd 0b 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0c 00 00 10 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELHud0P @ @	success or wait	3	71C6DD66	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	71C6DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE4FD.tmp	0	1307	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	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	44	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 51 75 6f 74 61 74 69 6f 6e 20 44 65 74 61 69 6c 73 2e 65 78 65	C:\Users\user\Desktop\Quotation Details.exe	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpE6C3.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	71C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 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(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	32	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327768	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	71C61B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72DDD72F	unknown
C:\Users\user\Desktop\Quotation Details.exe	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Users\user\Desktop\Quotation Details.exe	unknown	512	success or wait	1	72DDD72F	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	71C6646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **1968**, Parent PID: **5328**

General

Target ID:	4
Start time:	03:56:22
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpE4FD.tmp
Imagebase:	0xca0000
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\tmpE4FD.tmp	unknown	2	success or wait	1	CAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE4FD.tmp	unknown	1308	success or wait	1	CAABD9	ReadFile

Analysis Process: conhost.exe PID: **944**, Parent PID: **1968**

General

Target ID:	5
Start time:	03:56:22
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: schtasks.exe PID: **2108**, Parent PID: **5328**

General

Target ID:	6
Start time:	03:56:22
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpE6C3.tmp
Imagebase:	0xca0000
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\tmpE6C3.tmp	unknown	2	success or wait	1	CAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE6C3.tmp	unknown	1311	success or wait	1	CAABD9	ReadFile

Analysis Process: conhost.exe PID: **5644**, Parent PID: **2108**

General

Target ID:	7
Start time:	03:56:22
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: Quotation Details.exe PID: **2600**, Parent PID: **1088**

General

Target ID:	8
Start time:	03:56:24
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\Quotation Details.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Quotation Details.exe" 0
Imagebase:	0x190000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **1276**, Parent PID: **1088**

General

Target ID:	9
Start time:	03:56:24
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xe0000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 42%, 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	72E1CF06	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	72E1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7312C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: Quotation Details.exe PID: **5356**, Parent PID: **2600**

General	
Target ID:	10
Start time:	03:56:32
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\Quotation Details.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Quotation Details.exe
Imagebase:	0x3a0000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Quotation Details.exe PID: **5644**, Parent PID: **2600**

General	
Target ID:	11
Start time:	03:56:32
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\Quotation Details.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation Details.exe
Imagebase:	0x6c0000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.623117634.0000000003AA7000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.623117634.0000000003A9F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.623117634.0000000003A9F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.615605121.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.615605121.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.615605121.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.615605121.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.621560780.0000000002A41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.621560780.0000000002A41000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000B.00000002.621560780.0000000002A41000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **2404**, Parent PID: **1276**

General

Target ID:	12
Start time:	03:56:33
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xe0000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **2220**, Parent PID: **1276**

General

Target ID:	13
Start time:	03:56:33
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x5a0000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
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: 0000000D.00000002.622362871.0000000002B21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.622362871.0000000002B21000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.622362871.0000000002B21000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000D.00000002.623726899.0000000003B6B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **5692**, Parent PID: **3528**

General

Target ID:	14
Start time:	03:56:34
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xb90000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: dhcpmon.exe PID: **3616**, Parent PID: **5692**

General

Target ID:	15
Start time:	03:56:41
Start date:	31/05/2023

Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x4f0000
File size:	782336 bytes
MD5 hash:	5EC7A9D9A56FA3EB2D6F63A555969A37
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Disassembly

No disassembly