ID: 626643
Sample Name: 1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
Cookbook: default.jbs
Time: 18:52:25
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

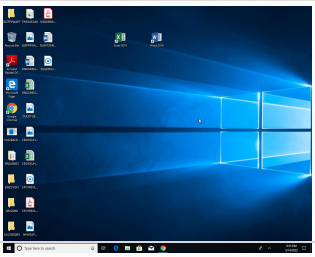
Windows Analysis Report

1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe

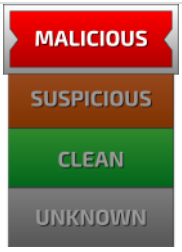
Overview

General Information

Sample Name:	1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
Analysis ID:	626643
MD5:	7564920df8fdac8..
SHA1:	7e5451c6de3e46..
SHA256:	1da2baedb633fd..
Tags:	exe NanoCore RAT
Infos:	



Detection



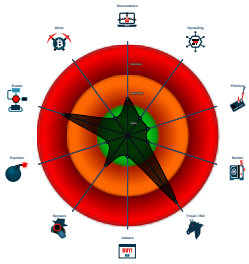
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- 1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe (PID: 6948 cmdline: "C:\Users\user\Desktop\1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe" MD5: 7564920DF8FDAC8A30144D4297173194)
- dhcpmon.exe (PID: 4684 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 7564920DF8FDAC8A30144D4297173194)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "9b13b828-50a9-4487-af40-2faff161",
  "Group": "Default",
  "Domain1": "6.tcp.ngrok.io",
  "Domain2": "6.tcp.ngrok.io",
  "Port": 10715,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "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"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected

Source	Rule	Description	Author	Strings
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfef5:$a: NanoCore 0xff05:$a: NanoCore 0x10139:$a: NanoCore 0x1014d:$a: NanoCore 0x1018d:$a: NanoCore 0xff54:$b: ClientPlugin 0x10156:$b: ClientPlugin 0x10196:$b: ClientPlugin 0x1007b:$c: ProjectData 0x10a82:$d: DESCrypto 0x1844e:$e: KeepAlive 0x1643c:$g: LogClientMessage 0x12637:$i: get_Connected 0x10db8:$j: #=q 0x10de8:$j: #=q 0x10e04:$j: #=q 0x10e34:$j: #=q 0x10e50:$j: #=q 0x10e6c:$j: #=q 0x10e9c:$j: #=q 0x10eb8:$j: #=q

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x1018d:$x1: NanoCore.ClientPluginHost 0x101ca:$x2: IClientNetworkHost 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xff05:$x1: NanoCore Client.exe 0x1018d:$x2: NanoCore.ClientPluginHost 0x117c6:$s1: PluginCommand 0x117ba:$s2: FileCommand 0x1266b:$s3: PipeExists 0x18422:$s4: PipeCreated 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	0xfef5:$x1: NanoCore Client 0xff05:$x1: NanoCore Client 0x1014d:$x2: NanoCore.ClientPlugin 0x1018d:$x3: NanoCore.ClientPluginHost 0x10142:$i1: IClientApp 0x10163:$i2: IClientData 0x1016f:$i3: IClientNetwork 0x1017e:$i4: IClientAppHost 0x101a7:$i5: IClientDataHost 0x101b7:$i6: IClientLoggingHost 0x101ca:$i7: IClientNetworkHost 0x101dd:$i8: IClientUIHost 0x101eb:$i9: IClientNameObjectCollection 0x10207:$i10: IClientReadOnlyNameObjectCollection 0xff54:$s1: ClientPlugin 0x10156:$s1: ClientPlugin 0x1064a:$s2: EndPoint 0x10653:$s3: IPAddress 0x1065d:$s4: IPEndPoint 0x12093:$s6: get_ClientSettings 0x12637:$s7: get_Connected
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfef5:$a: NanoCore 0xff05:$a: NanoCore 0x10139:$a: NanoCore 0x1014d:$a: NanoCore 0x1018d:$a: NanoCore 0xff54:$b: ClientPlugin 0x10156:$b: ClientPlugin 0x10196:$b: ClientPlugin 0x1007b:$c: ProjectData 0x10a82:$d: DESCrypto 0x1844e:$e: KeepAlive 0x1643c:$g: LogClientMessage 0x12637:$i: get_Connected 0x10db8:$j: #=q 0x10de8:$j: #=q 0x10e04:$j: #=q 0x10e34:$j: #=q 0x10e50:$j: #=q 0x10e6c:$j: #=q 0x10e9c:$j: #=q 0x10eb8:$j: #=q

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.267570909.0000000000A32000.00000002.00000001.01000000.00000005.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000000.267570909.0000000000A32000.00000002.00000001.01000000.00000005.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000000.267570909.0000000000A32000.00000002.00000001.01000000.00000005.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000000.242929781.0000000000302000.00000002.00000001.01000000.00000003.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.242929781.0000000000302000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.dhcpmon.exe.407e3c4.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
4.2.dhcpmon.exe.407e3c4.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
4.2.dhcpmon.exe.407e3c4.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
4.2.dhcpmon.exe.407e3c4.4.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xd978:$x2: NanoCore.ClientPlugin • 0xd9ad:$x3: NanoCore.ClientPluginHost • 0xd96c:$i2: IClientData • 0xd98e:$i3: IClientNetwork • 0xd99d:$i5: IClientDataHost • 0xd9c7:$i6: IClientLoggingHost • 0xd9da:$i7: IClientNetworkHost • 0xd9ed:$i8: IClientUIHost • 0xd9fb:$i9: IClientNameObjectCollection • 0xda17:$i10: IClientReadOnlyNameObjectCollection • 0xd76a:$s1: ClientPlugin • 0xd981:$s1: ClientPlugin • 0x129a2:$s6: get_ClientSettings
4.2.dhcpmon.exe.3053dc4.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 30 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549758107152816718 05/14/22-18:53:45.756170
SID:	2816718
Source Port:	49758
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549757107152025019 05/14/22-18:53:40.189537
SID:	2025019
Source Port:	49757
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.132.159.158

Timestamp:	192.168.2.33.132.159.15849794107152816766 05/14/22-18:54:36.688201
SID:	2816766
Source Port:	49794
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37

Timestamp:	192.168.2.33.141.210.3749806107152816766 05/14/22-18:54:41.730487
SID:	2816766
Source Port:	49806
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.21149848107152816766 05/14/22-18:54:51.648514
SID:	2816766
Source Port:	49848
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549854107152816766 05/14/22-18:55:01.842670
SID:	2816766
Source Port:	49854
Destination Port:	10715
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37	
Timestamp:	192.168.2.33.141.210.3749883107152025019 05/14/22-18:55:26.161126
SID:	2025019
Source Port:	49883
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.140.223.7	
Timestamp:	192.168.2.33.140.223.749740107152025019 05/14/22-18:53:30.583587
SID:	2025019
Source Port:	49740
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.21149765107152025019 05/14/22-18:54:00.755092
SID:	2025019
Source Port:	49765
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.140.223.7	
Timestamp:	192.168.2.33.140.223.749740107152816766 05/14/22-18:53:30.746005
SID:	2816766
Source Port:	49740
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37	
Timestamp:	192.168.2.33.141.210.3749806107152025019 05/14/22-18:54:41.230236
SID:	2025019
Source Port:	49806
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45	
Timestamp:	192.168.2.318.189.106.45497591071520250 19 05/14/22-18:53:50.228503
SID:	2025019
Source Port:	49759
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.21149756107152816766 05/14/22-18:53:35.773125
SID:	2816766
Source Port:	49756
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.177.1	
Timestamp:	192.168.2.33.141.177.149858107152025019 05/14/22-18:55:06.246494

SID:	2025019
Source Port:	49858
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549758107152025019 05/14/22-18:53:45.315185
SID:	2025019
Source Port:	49758
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.177.1

Timestamp:	192.168.2.33.141.177.149858107152816766 05/14/22-18:55:06.694095
SID:	2816766
Source Port:	49858
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549854107152025019 05/14/22-18:55:01.397157
SID:	2025019
Source Port:	49854
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549886107152025019 05/14/22-18:55:35.481238
SID:	2025019
Source Port:	49886
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.211497701071520250 19 05/14/22-18:54:06.080233
SID:	2025019
Source Port:	49770
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.211497811071520250 19 05/14/22-18:54:15.860094
SID:	2025019
Source Port:	49781
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37

Timestamp:	192.168.2.33.141.210.3749884107152025019 05/14/22-18:55:30.861568
SID:	2025019
Source Port:	49884
Destination Port:	10715
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.211497851071520250 19 05/14/22-18:54:25.617279
SID:	2025019
Source Port:	49785
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.211498361071528167 66 05/14/22-18:54:46.608305
SID:	2816766
Source Port:	49836
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45	
Timestamp:	192.168.2.318.189.106.45497911071528167 66 05/14/22-18:54:31.286610
SID:	2816766
Source Port:	49791
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.132.159.158	
Timestamp:	192.168.2.33.132.159.158498531071520250 19 05/14/22-18:54:56.252366
SID:	2025019
Source Port:	49853
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.211497831071520250 19 05/14/22-18:54:20.769932
SID:	2025019
Source Port:	49783
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.132.159.158	
Timestamp:	192.168.2.33.132.159.158498741071520250 19 05/14/22-18:55:11.701384
SID:	2025019
Source Port:	49874
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.211497561071520250 19 05/14/22-18:53:35.332411
SID:	2025019
Source Port:	49756
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45	
Timestamp:	192.168.2.318.189.106.45498801071520250 19 05/14/22-18:55:16.679672

SID:	2025019
Source Port:	49880
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549880107152816766 05/14/22-18:55:17.122336
SID:	2816766
Source Port:	49880
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549882107152025019 05/14/22-18:55:21.440941
SID:	2025019
Source Port:	49882
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.21149836107152816718 05/14/22-18:54:46.418129
SID:	2816718
Source Port:	49836
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549882107152816766 05/14/22-18:55:21.882674
SID:	2816766
Source Port:	49882
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37

Timestamp:	192.168.2.33.141.210.3749776107152025019 05/14/22-18:54:11.046665
SID:	2025019
Source Port:	49776
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.21149765107152816766 05/14/22-18:54:00.902736
SID:	2816766
Source Port:	49765
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37

Timestamp:	192.168.2.33.141.210.3749760107152816766 05/14/22-18:53:55.476894
SID:	2816766
Source Port:	49760
Destination Port:	10715
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.132.159.158	
Timestamp:	192.168.2.33.132.159.15849794107152025019 05/14/22-18:54:36.540422
SID:	2025019
Source Port:	49794
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.132.159.158	
Timestamp:	192.168.2.33.132.159.15849874107152816766 05/14/22-18:55:12.139699
SID:	2816766
Source Port:	49874
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45	
Timestamp:	192.168.2.318.189.106.4549757107152816766 05/14/22-18:53:40.555893
SID:	2816766
Source Port:	49757
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45	
Timestamp:	192.168.2.318.189.106.4549758107152816766 05/14/22-18:53:45.756170
SID:	2816766
Source Port:	49758
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.21149785107152816766 05/14/22-18:54:25.912977
SID:	2816766
Source Port:	49785
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37	
Timestamp:	192.168.2.33.141.210.3749776107152816766 05/14/22-18:54:11.487905
SID:	2816766
Source Port:	49776
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45	
Timestamp:	192.168.2.318.189.106.4549759107152816766 05/14/22-18:53:50.666342
SID:	2816766
Source Port:	49759
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.21149783107152816766 05/14/22-18:54:21.223616

SID:	2816766
Source Port:	49783
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37

Timestamp:	192.168.2.33.141.210.3749760107152025019 05/14/22-18:53:55.034238
SID:	2025019
Source Port:	49760
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.132.159.158

Timestamp:	192.168.2.33.132.159.15849853107152816766 05/14/22-18:54:56.699602
SID:	2816766
Source Port:	49853
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.21149781107152816766 05/14/22-18:54:16.302738
SID:	2816766
Source Port:	49781
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.21149770107152816766 05/14/22-18:54:06.525535
SID:	2816766
Source Port:	49770
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37

Timestamp:	192.168.2.33.141.210.3749884107152816766 05/14/22-18:55:31.304803
SID:	2816766
Source Port:	49884
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 18.189.106.45

Timestamp:	192.168.2.318.189.106.4549791107152025019 05/14/22-18:54:30.845080
SID:	2025019
Source Port:	49791
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211

Timestamp:	192.168.2.33.141.142.21149836107152025019 05/14/22-18:54:46.122377
SID:	2025019
Source Port:	49836
Destination Port:	10715
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 3.141.142.211	
Timestamp:	192.168.2.33.141.142.21149848107152025019 05/14/22-18:54:51.048070
SID:	2025019
Source Port:	49848
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 3.141.210.37	
Timestamp:	192.168.2.33.141.210.3749883107152816766 05/14/22-18:55:26.602738
SID:	2816766
Source Port:	49883
Destination Port:	10715
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

- Yara detected Nanocore RAT

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

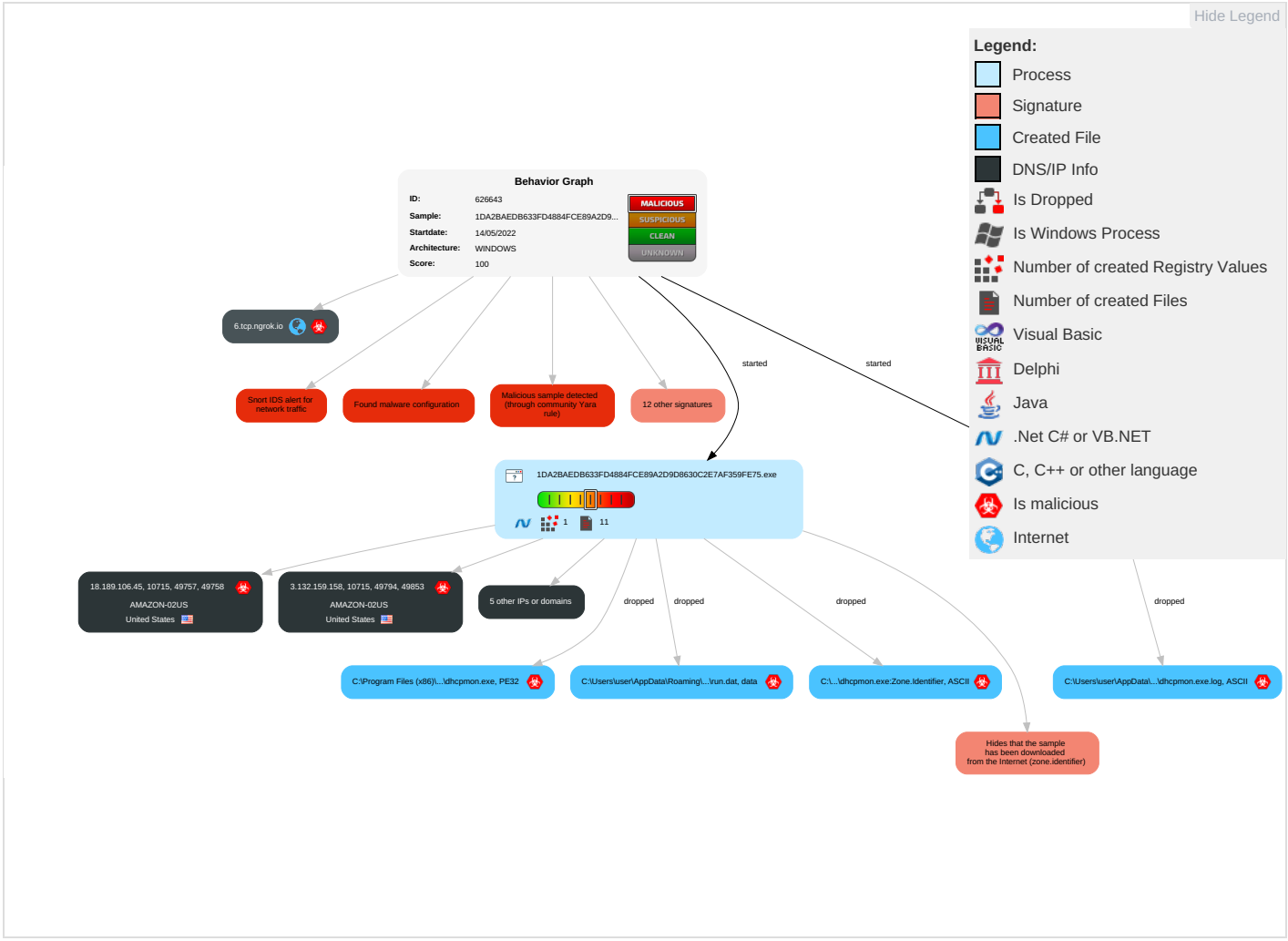
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	2 Process Injection	2 Masquerading	1 1 Input Capture	1 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	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)	2 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	2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 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	1 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
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	83%	Metadefender		Browse
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	83%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe.300000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
4.0.dhcpmon.exe.a30000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
4.2.dhcpmon.exe.a30000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
6.tcp.ngrok.io	100%	Avira URL Cloud	malware	

Domains and IPs

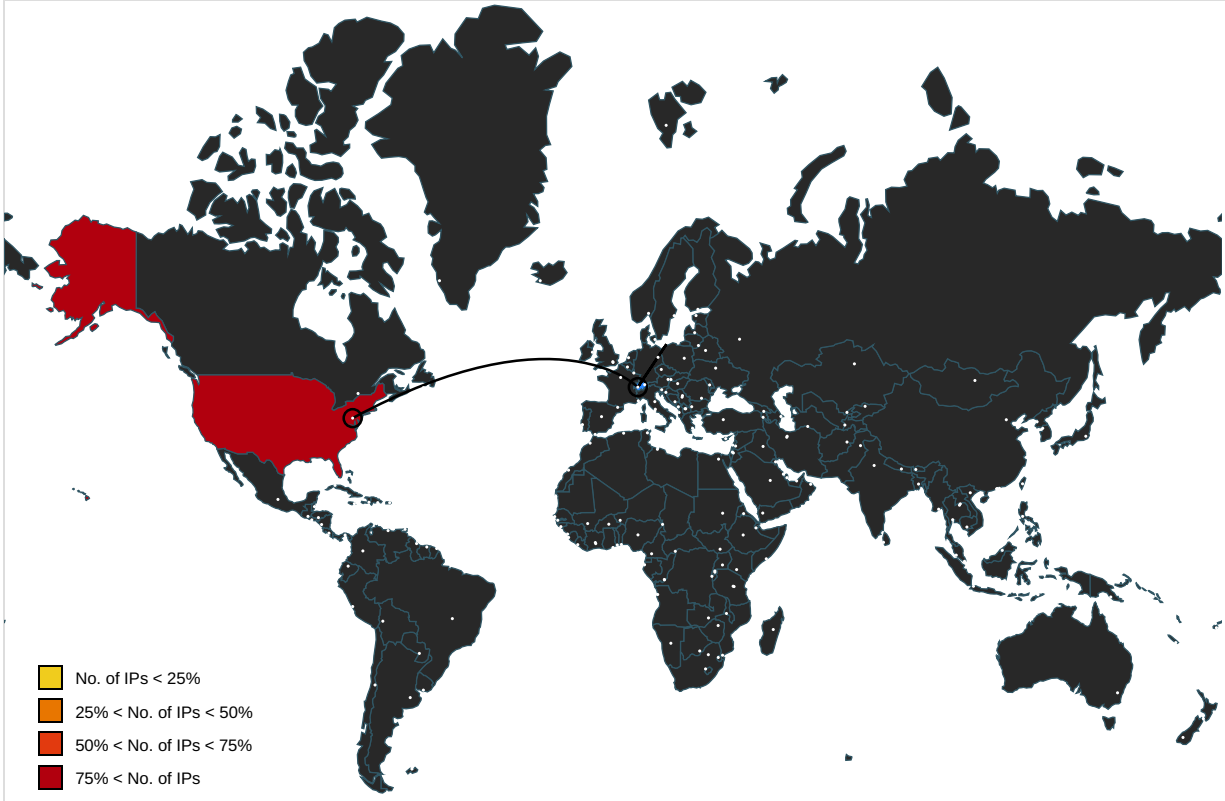
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
6.tcp.ngrok.io	3.140.223.7	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
6.tcp.ngrok.io	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.141.142.211	unknown	United States		16509	AMAZON-02US	true
18.189.106.45	unknown	United States		16509	AMAZON-02US	true
3.141.210.37	unknown	United States		16509	AMAZON-02US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.140.223.7	6.tcp.ngrok.io	United States		16509	AMAZON-02US	true
3.141.177.1	unknown	United States		16509	AMAZON-02US	true
3.132.159.158	unknown	United States		16509	AMAZON-02US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626643
Start date and time: 14/05/202218:52:25	2022-05-14 18:52:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@2/4@26/7
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target 1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe, PID 6948 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- VT rate limit hit for: 1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe

Simulations

Behavior and APIs

Time	Type	Description
18:53:28	API Interceptor	1000x Sleep call for process: 1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe modified
18:53:29	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.44673871085536
Encrypted:	false
SSDEEP:	6144:gLV6Bta6dtJmakIM5HlWUu5LYkO0TrWSB:gLV6BtpmkIM5LYkO0TKM
MD5:	7564920DF8FDAC8A30144D4297173194
SHA1:	7E5451C6DE3E46983C22AB6FE70EB0C6E5FC21DA
SHA-256:	1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE7519F677AD64BCC162A61
SHA-512:	A208A85DAB10B37E344D5EBED56C05DD09C93EACC6AAAE610DD5D4E8E395A3788CBE6342C7000A27CBDCBCABED6E5043FABF5D796853794A9498AFDF0332D6F6
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 83%, Browse • Antivirus: ReversingLabs, Detection: 98%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. .....8...W.... ..p]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...p]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

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

Process:	C:\Users\user\Desktop\1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

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

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

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

Process:	C:\Users\user\Desktop\1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Jtn:jn
MD5:	24DE9846E6AE08C5DCA9BCDA9F509FC1
SHA1:	CFA73A7289F9EC1FEC3DCDAB3B7D6FC788BF52B7
SHA-256:	0EA4EE35E4DB371C1C0ACCC8D42C119750B93519D77263572574AD7EE2321E5B
SHA-512:	BF56D6F04A2402E3B064ACE5B2FB0B3B8E201EBA90BF713430347063CE4D5736F23C07652B3E5FD0DC60BB533AF463A136BBB64DCC6ACE6EE98F7104A9D82B52
Malicious:	**true**
Reputation:	low
Preview:	..Z..6.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Entropy (8bit):	7.44673871085536
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
File size:	207360
MD5:	7564920df8fdac8a30144d4297173194
SHA1:	7e5451c6de3e46983c22ab6fe70eb0c6e5fc21da
SHA256:	1da2baedb633fd4884fce89a2d9d8630c2e7af359fe7519f677ad64bcc162a61
SHA512:	a208a85dab10b37e344d5ebed56c05dd09c93eacc6aaae610dd5d4e8e395a3788cbe6342c7000a27cbdcbcabed6e5043fabf5d796853794a9498afdf0332d6f6
SSDEEP:	6144:gLV6Bta6dtJmakIM5HlWUu5LYkO0TrWSB:gLV6BtpmkIlM5LYkO0TKM
TLSH:	4914BF5677E94A2FE2DE86B9602211128379C2E3E8C3F7DE28D454F78B267E406071D3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x15d70	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.594503837719	data	6.59807178823	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15d70	0x15e00	False	0.999352678571	data	7.99767001734	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x15d18	TIM image, (20535,52663)		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

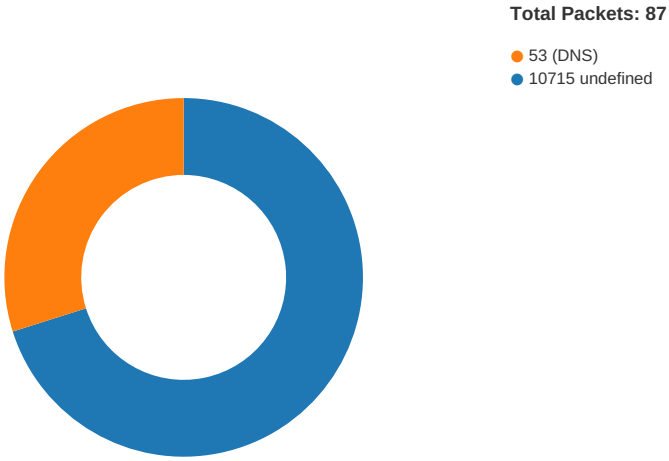
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.318.189.106.45 49758107152816718 05/14/22-18:53:45.756170	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49758	10715	192.168.2.3	18.189.106.45
192.168.2.318.189.106.45 49757107152025019 05/14/22-18:53:40.189537	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	10715	192.168.2.3	18.189.106.45
192.168.2.33.132.159.158 49794107152816766 05/14/22-18:54:36.688201	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49794	10715	192.168.2.3	3.132.159.158
192.168.2.33.141.210.374 9806107152816766 05/14/22-18:54:41.730487	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49806	10715	192.168.2.3	3.141.210.37
192.168.2.33.141.142.211 49848107152816766 05/14/22-18:54:51.648514	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49848	10715	192.168.2.3	3.141.142.211
192.168.2.318.189.106.45 49854107152816766 05/14/22-18:55:01.842670	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49854	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.210.374 9883107152025019 05/14/22-18:55:26.161126	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49883	10715	192.168.2.3	3.141.210.37
192.168.2.33.140.223.749 740107152025019 05/14/22-18:53:30.583587	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	10715	192.168.2.3	3.140.223.7
192.168.2.33.141.142.211 49765107152025019 05/14/22-18:54:00.755092	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	10715	192.168.2.3	3.141.142.211
192.168.2.33.140.223.749 740107152816766 05/14/22-18:53:30.746005	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49740	10715	192.168.2.3	3.140.223.7
192.168.2.33.141.210.374 9806107152025019 05/14/22-18:54:41.230236	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49806	10715	192.168.2.3	3.141.210.37
192.168.2.318.189.106.45 49759107152025019 05/14/22-18:53:50.228503	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.142.211 49756107152816766 05/14/22-18:53:35.773125	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49756	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.177.149 858107152025019 05/14/22-18:55:06.246494	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49858	10715	192.168.2.3	3.141.177.1
192.168.2.318.189.106.45 49758107152025019 05/14/22-18:53:45.315185	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.177.149 858107152816766 05/14/22-18:55:06.694095	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49858	10715	192.168.2.3	3.141.177.1

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.318.189.106.45 49854107152025019 05/14/22-18:55:01.397157	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49854	10715	192.168.2.3	18.189.106.45
192.168.2.318.189.106.45 49886107152025019 05/14/22-18:55:35.481238	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49886	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.142.211 49770107152025019 05/14/22-18:54:06.080233	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.142.211 49781107152025019 05/14/22-18:54:15.860094	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.210.374 9884107152025019 05/14/22-18:55:30.861568	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49884	10715	192.168.2.3	3.141.210.37
192.168.2.33.141.142.211 49785107152025019 05/14/22-18:54:25.617279	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.142.211 49836107152816766 05/14/22-18:54:46.608305	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49836	10715	192.168.2.3	3.141.142.211
192.168.2.318.189.106.45 49791107152816766 05/14/22-18:54:31.286610	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49791	10715	192.168.2.3	18.189.106.45
192.168.2.33.132.159.158 49853107152025019 05/14/22-18:54:56.252366	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49853	10715	192.168.2.3	3.132.159.158
192.168.2.33.141.142.211 49783107152025019 05/14/22-18:54:20.769932	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	10715	192.168.2.3	3.141.142.211
192.168.2.33.132.159.158 49874107152025019 05/14/22-18:55:11.701384	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49874	10715	192.168.2.3	3.132.159.158
192.168.2.33.141.142.211 49756107152025019 05/14/22-18:53:35.332411	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	10715	192.168.2.3	3.141.142.211
192.168.2.318.189.106.45 49880107152025019 05/14/22-18:55:16.679672	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49880	10715	192.168.2.3	18.189.106.45
192.168.2.318.189.106.45 49880107152816766 05/14/22-18:55:17.122336	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49880	10715	192.168.2.3	18.189.106.45
192.168.2.318.189.106.45 49882107152025019 05/14/22-18:55:21.440941	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49882	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.142.211 49836107152816718 05/14/22-18:54:46.418129	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49836	10715	192.168.2.3	3.141.142.211
192.168.2.318.189.106.45 49882107152816766 05/14/22-18:55:21.882674	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49882	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.210.374 9776107152025019 05/14/22-18:54:11.046665	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	10715	192.168.2.3	3.141.210.37
192.168.2.33.141.142.211 49765107152816766 05/14/22-18:54:00.902736	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49765	10715	192.168.2.3	3.141.142.211

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.33.141.210.3749760107152816766 05/14/22-18:53:55.476894	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49760	10715	192.168.2.3	3.141.210.37
192.168.2.33.132.159.1584979410715202501 9 05/14/22-18:54:36.540422	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	10715	192.168.2.3	3.132.159.158
192.168.2.33.132.159.1584987410715281676 6 05/14/22-18:55:12.139699	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49874	10715	192.168.2.3	3.132.159.158
192.168.2.318.189.106.454975710715281676 6 05/14/22-18:53:40.555893	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49757	10715	192.168.2.3	18.189.106.45
192.168.2.318.189.106.454975810715281676 6 05/14/22-18:53:45.756170	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49758	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.142.2114978510715281676 6 05/14/22-18:54:25.912977	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49785	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.210.3749776107152816766 05/14/22-18:54:11.487905	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49776	10715	192.168.2.3	3.141.210.37
192.168.2.318.189.106.454975910715281676 6 05/14/22-18:53:50.666342	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49759	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.142.2114978310715281676 6 05/14/22-18:54:21.223616	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49783	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.210.3749760107152025019 05/14/22-18:53:55.034238	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	10715	192.168.2.3	3.141.210.37
192.168.2.33.132.159.1584985310715281676 6 05/14/22-18:54:56.699602	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49853	10715	192.168.2.3	3.132.159.158
192.168.2.33.141.142.2114978110715281676 6 05/14/22-18:54:16.302738	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49781	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.142.2114977010715281676 6 05/14/22-18:54:06.525535	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49770	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.210.3749884107152816766 05/14/22-18:55:31.304803	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49884	10715	192.168.2.3	3.141.210.37
192.168.2.318.189.106.454979110715202501 9 05/14/22-18:54:30.845080	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	10715	192.168.2.3	18.189.106.45
192.168.2.33.141.142.2114983610715202501 9 05/14/22-18:54:46.122377	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.142.2114984810715202501 9 05/14/22-18:54:51.048070	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	10715	192.168.2.3	3.141.142.211
192.168.2.33.141.210.3749883107152816766 05/14/22-18:55:26.602738	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49883	10715	192.168.2.3	3.141.210.37

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 18:53:30.152717113 CEST	49740	10715	192.168.2.3	3.140.223.7
May 14, 2022 18:53:30.300458908 CEST	10715	49740	3.140.223.7	192.168.2.3
May 14, 2022 18:53:30.300592899 CEST	49740	10715	192.168.2.3	3.140.223.7
May 14, 2022 18:53:30.583586931 CEST	49740	10715	192.168.2.3	3.140.223.7
May 14, 2022 18:53:30.731373072 CEST	10715	49740	3.140.223.7	192.168.2.3
May 14, 2022 18:53:30.731479883 CEST	49740	10715	192.168.2.3	3.140.223.7
May 14, 2022 18:53:30.745915890 CEST	10715	49740	3.140.223.7	192.168.2.3
May 14, 2022 18:53:30.746005058 CEST	49740	10715	192.168.2.3	3.140.223.7
May 14, 2022 18:53:30.752690077 CEST	49740	10715	192.168.2.3	3.140.223.7
May 14, 2022 18:53:30.893910885 CEST	10715	49740	3.140.223.7	192.168.2.3
May 14, 2022 18:53:30.894033909 CEST	49740	10715	192.168.2.3	3.140.223.7
May 14, 2022 18:53:35.177712917 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.325093985 CEST	10715	49756	3.141.142.211	192.168.2.3
May 14, 2022 18:53:35.325269938 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.332411051 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.479594946 CEST	10715	49756	3.141.142.211	192.168.2.3
May 14, 2022 18:53:35.480998039 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.628302097 CEST	10715	49756	3.141.142.211	192.168.2.3
May 14, 2022 18:53:35.628876925 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.771130085 CEST	10715	49756	3.141.142.211	192.168.2.3
May 14, 2022 18:53:35.773124933 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.773258924 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.776134968 CEST	10715	49756	3.141.142.211	192.168.2.3
May 14, 2022 18:53:35.776266098 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:35.920591116 CEST	10715	49756	3.141.142.211	192.168.2.3
May 14, 2022 18:53:35.920778036 CEST	49756	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:53:40.026853085 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:40.174282074 CEST	10715	49757	18.189.106.45	192.168.2.3
May 14, 2022 18:53:40.174491882 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:40.189537048 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:40.336873055 CEST	10715	49757	18.189.106.45	192.168.2.3
May 14, 2022 18:53:40.336997986 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:40.484273911 CEST	10715	49757	18.189.106.45	192.168.2.3
May 14, 2022 18:53:40.555892944 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:40.629710913 CEST	10715	49757	18.189.106.45	192.168.2.3
May 14, 2022 18:53:40.629822016 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:40.631099939 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:40.703073025 CEST	10715	49757	18.189.106.45	192.168.2.3
May 14, 2022 18:53:40.703206062 CEST	49757	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.166917086 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.314317942 CEST	10715	49758	18.189.106.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 18:53:45.314440012 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.315185070 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.462436914 CEST	10715	49758	18.189.106.45	192.168.2.3
May 14, 2022 18:53:45.463409901 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.610654116 CEST	10715	49758	18.189.106.45	192.168.2.3
May 14, 2022 18:53:45.618048906 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.755908012 CEST	10715	49758	18.189.106.45	192.168.2.3
May 14, 2022 18:53:45.756170034 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.756222963 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.765223980 CEST	10715	49758	18.189.106.45	192.168.2.3
May 14, 2022 18:53:45.767869949 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:45.903568029 CEST	10715	49758	18.189.106.45	192.168.2.3
May 14, 2022 18:53:45.905920982 CEST	49758	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.075531006 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.223118067 CEST	10715	49759	18.189.106.45	192.168.2.3
May 14, 2022 18:53:50.223277092 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.228502989 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.375870943 CEST	10715	49759	18.189.106.45	192.168.2.3
May 14, 2022 18:53:50.376728058 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.524233103 CEST	10715	49759	18.189.106.45	192.168.2.3
May 14, 2022 18:53:50.524324894 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.664855957 CEST	10715	49759	18.189.106.45	192.168.2.3
May 14, 2022 18:53:50.666342020 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.666410923 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.671622992 CEST	10715	49759	18.189.106.45	192.168.2.3
May 14, 2022 18:53:50.673928976 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:50.813819885 CEST	10715	49759	18.189.106.45	192.168.2.3
May 14, 2022 18:53:50.814275980 CEST	49759	10715	192.168.2.3	18.189.106.45
May 14, 2022 18:53:54.885710001 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:53:55.033107042 CEST	10715	49760	3.141.210.37	192.168.2.3
May 14, 2022 18:53:55.033243895 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:53:55.034238100 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:53:55.181597948 CEST	10715	49760	3.141.210.37	192.168.2.3
May 14, 2022 18:53:55.181685925 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:53:55.329044104 CEST	10715	49760	3.141.210.37	192.168.2.3
May 14, 2022 18:53:55.329144955 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:53:55.476773977 CEST	10715	49760	3.141.210.37	192.168.2.3
May 14, 2022 18:53:55.476893902 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:53:55.478843927 CEST	10715	49760	3.141.210.37	192.168.2.3
May 14, 2022 18:53:55.478924990 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:53:55.479059935 CEST	49760	10715	192.168.2.3	3.141.210.37
May 14, 2022 18:54:00.582742929 CEST	49765	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:00.730499029 CEST	10715	49765	3.141.142.211	192.168.2.3
May 14, 2022 18:54:00.730712891 CEST	49765	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:00.755091906 CEST	49765	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:00.902534008 CEST	10715	49765	3.141.142.211	192.168.2.3
May 14, 2022 18:54:00.902735949 CEST	49765	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:01.050062895 CEST	10715	49765	3.141.142.211	192.168.2.3
May 14, 2022 18:54:01.178420067 CEST	10715	49765	3.141.142.211	192.168.2.3
May 14, 2022 18:54:01.353086948 CEST	49765	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:01.642544985 CEST	49765	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:05.931350946 CEST	49770	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:06.078870058 CEST	10715	49770	3.141.142.211	192.168.2.3
May 14, 2022 18:54:06.079674959 CEST	49770	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:06.080233097 CEST	49770	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:06.227596998 CEST	10715	49770	3.141.142.211	192.168.2.3
May 14, 2022 18:54:06.230441093 CEST	49770	10715	192.168.2.3	3.141.142.211
May 14, 2022 18:54:06.377821922 CEST	10715	49770	3.141.142.211	192.168.2.3
May 14, 2022 18:54:06.377979040 CEST	49770	10715	192.168.2.3	3.141.142.211

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 18:53:30.123356104 CEST	57421	53	192.168.2.3	8.8.8.8
May 14, 2022 18:53:30.139904022 CEST	53	57421	8.8.8.8	192.168.2.3
May 14, 2022 18:53:35.043431997 CEST	65358	53	192.168.2.3	8.8.8.8
May 14, 2022 18:53:35.062048912 CEST	53	65358	8.8.8.8	192.168.2.3
May 14, 2022 18:53:39.983046055 CEST	49873	53	192.168.2.3	8.8.8.8
May 14, 2022 18:53:40.001665115 CEST	53	49873	8.8.8.8	192.168.2.3
May 14, 2022 18:53:45.130386114 CEST	53802	53	192.168.2.3	8.8.8.8
May 14, 2022 18:53:45.148720980 CEST	53	53802	8.8.8.8	192.168.2.3
May 14, 2022 18:53:50.055612087 CEST	65266	53	192.168.2.3	8.8.8.8
May 14, 2022 18:53:50.074321032 CEST	53	65266	8.8.8.8	192.168.2.3
May 14, 2022 18:53:54.865468025 CEST	63332	53	192.168.2.3	8.8.8.8
May 14, 2022 18:53:54.884104013 CEST	53	63332	8.8.8.8	192.168.2.3
May 14, 2022 18:54:00.538901091 CEST	51391	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:00.557221889 CEST	53	51391	8.8.8.8	192.168.2.3
May 14, 2022 18:54:05.910094976 CEST	52985	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:05.930022001 CEST	53	52985	8.8.8.8	192.168.2.3
May 14, 2022 18:54:10.878411055 CEST	50778	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:10.896574020 CEST	53	50778	8.8.8.8	192.168.2.3
May 14, 2022 18:54:15.692712069 CEST	59390	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:15.709459066 CEST	53	59390	8.8.8.8	192.168.2.3
May 14, 2022 18:54:20.602340937 CEST	64996	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:20.620956898 CEST	53	64996	8.8.8.8	192.168.2.3
May 14, 2022 18:54:25.447983980 CEST	52096	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:25.466384888 CEST	53	52096	8.8.8.8	192.168.2.3
May 14, 2022 18:54:30.676806927 CEST	49844	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:30.695350885 CEST	53	49844	8.8.8.8	192.168.2.3
May 14, 2022 18:54:36.010186911 CEST	49723	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:36.031011105 CEST	53	49723	8.8.8.8	192.168.2.3
May 14, 2022 18:54:41.064217091 CEST	61877	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:41.080579042 CEST	53	61877	8.8.8.8	192.168.2.3
May 14, 2022 18:54:45.954760075 CEST	61555	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:45.973352909 CEST	53	61555	8.8.8.8	192.168.2.3
May 14, 2022 18:54:50.838273048 CEST	51557	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:50.856714964 CEST	53	51557	8.8.8.8	192.168.2.3
May 14, 2022 18:54:56.082479000 CEST	52487	53	192.168.2.3	8.8.8.8
May 14, 2022 18:54:56.100958109 CEST	53	52487	8.8.8.8	192.168.2.3
May 14, 2022 18:55:01.203088045 CEST	51994	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:01.223702908 CEST	53	51994	8.8.8.8	192.168.2.3
May 14, 2022 18:55:06.072969913 CEST	58950	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:06.091731071 CEST	53	58950	8.8.8.8	192.168.2.3
May 14, 2022 18:55:11.520415068 CEST	53883	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:11.539225101 CEST	53	53883	8.8.8.8	192.168.2.3
May 14, 2022 18:55:16.511949062 CEST	59065	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:16.530073881 CEST	53	59065	8.8.8.8	192.168.2.3
May 14, 2022 18:55:21.275295019 CEST	64589	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:21.291465998 CEST	53	64589	8.8.8.8	192.168.2.3
May 14, 2022 18:55:25.990437984 CEST	64934	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:26.008608103 CEST	53	64934	8.8.8.8	192.168.2.3
May 14, 2022 18:55:30.696547031 CEST	55795	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:30.712841988 CEST	53	55795	8.8.8.8	192.168.2.3
May 14, 2022 18:55:35.315671921 CEST	55269	53	192.168.2.3	8.8.8.8
May 14, 2022 18:55:35.332572937 CEST	53	55269	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 18:53:30.123356104 CEST	192.168.2.3	8.8.8.8	0xbdbb	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 18:53:35.043431997 CEST	192.168.2.3	8.8.8.8	0x8498	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:53:39.983046055 CEST	192.168.2.3	8.8.8.8	0xbd83	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:53:45.130386114 CEST	192.168.2.3	8.8.8.8	0x78a9	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:53:50.055612087 CEST	192.168.2.3	8.8.8.8	0x8955	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:53:54.865468025 CEST	192.168.2.3	8.8.8.8	0xb083	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:00.538901091 CEST	192.168.2.3	8.8.8.8	0xbc15	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:05.910094976 CEST	192.168.2.3	8.8.8.8	0x5516	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:10.878411055 CEST	192.168.2.3	8.8.8.8	0xf614	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:15.692712069 CEST	192.168.2.3	8.8.8.8	0x4c7f	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:20.602340937 CEST	192.168.2.3	8.8.8.8	0xd61f	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:25.447983980 CEST	192.168.2.3	8.8.8.8	0x6a3e	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:30.676806927 CEST	192.168.2.3	8.8.8.8	0xec3b	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:36.010186911 CEST	192.168.2.3	8.8.8.8	0xe2ac	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:41.064217091 CEST	192.168.2.3	8.8.8.8	0x4a9c	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:45.954760075 CEST	192.168.2.3	8.8.8.8	0xab74	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:50.838273048 CEST	192.168.2.3	8.8.8.8	0xf6e8	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:54:56.082479000 CEST	192.168.2.3	8.8.8.8	0x64f0	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:01.203088045 CEST	192.168.2.3	8.8.8.8	0xebf4	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:06.072969913 CEST	192.168.2.3	8.8.8.8	0x67d5	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:11.520415068 CEST	192.168.2.3	8.8.8.8	0x9d90	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:16.511949062 CEST	192.168.2.3	8.8.8.8	0x4a6	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:21.275295019 CEST	192.168.2.3	8.8.8.8	0xcd3e	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:25.990437984 CEST	192.168.2.3	8.8.8.8	0xaee9	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:30.696547031 CEST	192.168.2.3	8.8.8.8	0x371a	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)
May 14, 2022 18:55:35.315671921 CEST	192.168.2.3	8.8.8.8	0x6b7d	Standard query (0)	6.tcp.ngrok.io	A (IP address)	IN (0x0001)

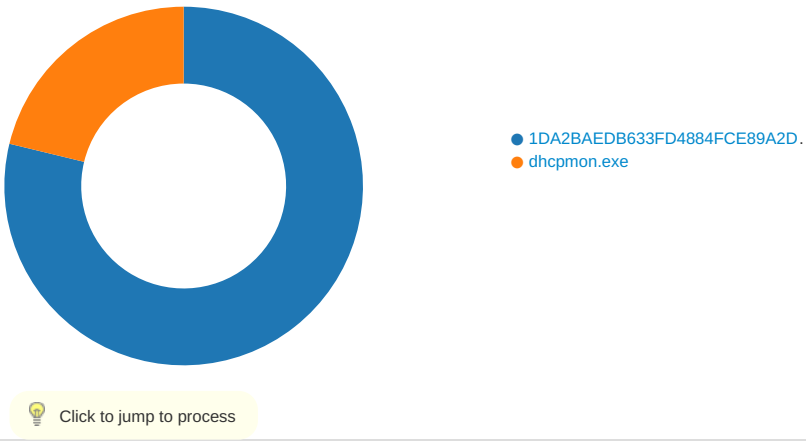
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 18:53:30.139904022 CEST	8.8.8.8	192.168.2.3	0xbdbb	No error (0)	6.tcp.ngrok.io		3.140.223.7	A (IP address)	IN (0x0001)
May 14, 2022 18:53:35.062048912 CEST	8.8.8.8	192.168.2.3	0x8498	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)
May 14, 2022 18:53:40.001665115 CEST	8.8.8.8	192.168.2.3	0xbd83	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)
May 14, 2022 18:53:45.148720980 CEST	8.8.8.8	192.168.2.3	0x78a9	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)
May 14, 2022 18:53:50.074321032 CEST	8.8.8.8	192.168.2.3	0x8955	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)
May 14, 2022 18:53:54.884104013 CEST	8.8.8.8	192.168.2.3	0xb083	No error (0)	6.tcp.ngrok.io		3.141.210.37	A (IP address)	IN (0x0001)
May 14, 2022 18:54:00.557221889 CEST	8.8.8.8	192.168.2.3	0xbc15	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)
May 14, 2022 18:54:05.930022001 CEST	8.8.8.8	192.168.2.3	0x5516	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 18:54:10.896574020 CEST	8.8.8.8	192.168.2.3	0xf614	No error (0)	6.tcp.ngrok.io		3.141.210.37	A (IP address)	IN (0x0001)
May 14, 2022 18:54:15.709459066 CEST	8.8.8.8	192.168.2.3	0x4c7f	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)
May 14, 2022 18:54:20.620956898 CEST	8.8.8.8	192.168.2.3	0xd61f	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)
May 14, 2022 18:54:25.466384888 CEST	8.8.8.8	192.168.2.3	0x6a3e	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)
May 14, 2022 18:54:30.695350885 CEST	8.8.8.8	192.168.2.3	0xec3b	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)
May 14, 2022 18:54:36.031011105 CEST	8.8.8.8	192.168.2.3	0xe2ac	No error (0)	6.tcp.ngrok.io		3.132.159.158	A (IP address)	IN (0x0001)
May 14, 2022 18:54:41.080579042 CEST	8.8.8.8	192.168.2.3	0x4a9c	No error (0)	6.tcp.ngrok.io		3.141.210.37	A (IP address)	IN (0x0001)
May 14, 2022 18:54:45.973352909 CEST	8.8.8.8	192.168.2.3	0xab74	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)
May 14, 2022 18:54:50.856714964 CEST	8.8.8.8	192.168.2.3	0xf6e8	No error (0)	6.tcp.ngrok.io		3.141.142.211	A (IP address)	IN (0x0001)
May 14, 2022 18:54:56.100958109 CEST	8.8.8.8	192.168.2.3	0x64f0	No error (0)	6.tcp.ngrok.io		3.132.159.158	A (IP address)	IN (0x0001)
May 14, 2022 18:55:01.223702908 CEST	8.8.8.8	192.168.2.3	0xebf4	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)
May 14, 2022 18:55:06.091731071 CEST	8.8.8.8	192.168.2.3	0x67d5	No error (0)	6.tcp.ngrok.io		3.141.177.1	A (IP address)	IN (0x0001)
May 14, 2022 18:55:11.539225101 CEST	8.8.8.8	192.168.2.3	0x9d90	No error (0)	6.tcp.ngrok.io		3.132.159.158	A (IP address)	IN (0x0001)
May 14, 2022 18:55:16.530073881 CEST	8.8.8.8	192.168.2.3	0x4a6	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)
May 14, 2022 18:55:21.291465998 CEST	8.8.8.8	192.168.2.3	0xcd3e	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)
May 14, 2022 18:55:26.008608103 CEST	8.8.8.8	192.168.2.3	0xaee9	No error (0)	6.tcp.ngrok.io		3.141.210.37	A (IP address)	IN (0x0001)
May 14, 2022 18:55:30.712841988 CEST	8.8.8.8	192.168.2.3	0x371a	No error (0)	6.tcp.ngrok.io		3.141.210.37	A (IP address)	IN (0x0001)
May 14, 2022 18:55:35.332572937 CEST	8.8.8.8	192.168.2.3	0x6b7d	No error (0)	6.tcp.ngrok.io		18.189.106.45	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: 1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe PID: **6948**, Parent PID: **6012**

General

Target ID:	0
Start time:	18:53:25
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe"
Imagebase:	0x300000
File size:	207360 bytes
MD5 hash:	7564920DF8FDAC8A30144D4297173194
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.242929781.0000000000302000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.242929781.0000000000302000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.242929781.0000000000302000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726360AC	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	726360AC	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	4B30D15	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	4B30E0F	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	4B30D15	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	4B31094	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	4B31094	CopyFileW
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	4B30D15	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4B30D15	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726360AC	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	726360AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1DA2BAEDB633FD4884FCE89A2D9D8630C2E7AF359FE75.exe:Zone.Identifier	success or wait	1	4B31265	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	03 fd 5a fd 15 36 fd 48	Z6H	success or wait	1	4B30FC7	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 60 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'T` @	success or wait	2	4B31094	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	4B31094	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72665544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72665544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72668738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7270BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7270BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1DA2BAED B633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	unknown	4096	success or wait	1	7270BF06	unknown
C:\Users\user\Desktop\1DA2BAED B633FD4884FCE89A2D9D8630C2E7AF359FE75.exe	unknown	512	success or wait	1	7270BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	4095	success or wait	1	72665544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	8175	end of file	1	72665544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	4096	end of file	1	4B30FC7	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	4B31186	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **4684**, Parent PID: **3968**

General

Target ID:	4
Start time:	18:53:37
Start date:	14/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xa30000
File size:	207360 bytes
MD5 hash:	7564920DF8FDAC8A30144D4297173194
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.267570909.0000000000A32000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.267570909.0000000000A32000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.267570909.0000000000A32000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.286197022.0000000004031000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.286197022.0000000004031000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.286128721.0000000003031000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.286128721.0000000003031000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.285634821.0000000000A32000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.285634821.0000000000A32000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.285634821.0000000000A32000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 83%, Metadefender, Browse • Detection: 98%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726360AC	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	726360AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	726234A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	7290A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72665544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72665544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72668738	ReadFile

Disassembly

No disassembly