ID: 880361
Sample Name:
sqeCz4tgdW.exe
Cookbook: default.jbs
Time: 03:16:15
Date: 02/06/2023
Version: 37.1.0 Beryl

Table of Contents

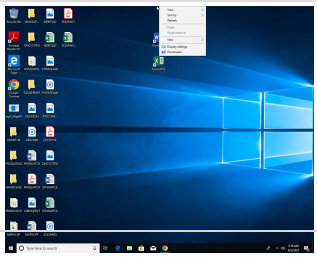
Windows Analysis Report

sqeCz4tgdW.exe

Overview

General Information

Sample Name:	sqeCz4tgdW.exe
Original Sample Name:	0cea4eaf61419..
Analysis ID:	880361
MD5:	0cea4eaf61419..
SHA1:	1f5259a6eeef5...
SHA256:	597475447158...
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

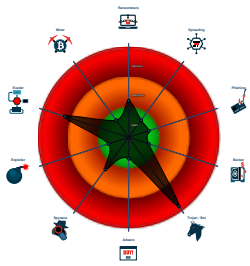
Nanocore

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- sqeCz4tgdW.exe (PID: 7000 cmdline: C:\Users\user\Desktop\sqeCz4tgdW.exe MD5: 0CEA4EAF614191A2CF51ABD70A672ED9)
- dhcpmon.exe (PID: 3568 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 0CEA4EAF614191A2CF51ABD70A672ED9)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	http://https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/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": "95d7519b-29ef-446d-9925-48c3abcd",
  "Group": "Default",
  "Domain1": "4.tcp.ngrok.io",
  "Domain2": "4.tcp.ngrok.io",
  "Port": 17403,
  "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
sqeCz4tgdW.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
sqeCz4tgdW.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
sqeCz4tgdW.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
sqeCz4tgdW.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
sqeCz4tgdW.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
00000001.00000002.385393945.0000000003AF1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 22 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.sqeCz4tgdW.exe.5620000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
0.2.sqeCz4tgdW.exe.5620000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0.2.sqeCz4tgdW.exe.5620000.3.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
0.2.sqeCz4tgdW.exe.5620000.3.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
1.2.dhcpmon.exe.3b429ed.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c38:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c65:$x2: IClientNetworkHost

Click to see the 49 entries

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49

Timestamp:	192.168.2.73.131.147.4949711174032816766 06/02/23-03:18:14.807235
SID:	2816766
Source Port:	49711
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135

Timestamp:	192.168.2.73.22.15.13549701174032816766 06/02/23-03:17:24.631045
SID:	2816766
Source Port:	49701
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135

Timestamp:	192.168.2.73.22.15.13549712174032816766 06/02/23-03:18:19.558845
SID:	2816766
Source Port:	49712
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49

Timestamp:	192.168.2.73.131.147.4949722174032816766 06/02/23-03:19:11.880129
SID:	2816766
Source Port:	49722
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49

Timestamp:	192.168.2.73.131.147.4949713174032816766 06/02/23-03:18:24.437024
SID:	2816766
Source Port:	49713

Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.13549710174032816766 06/02/23-03:18:10.096340
SID:	2816766
Source Port:	49710
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949720174032816766 06/02/23-03:19:01.687305
SID:	2816766
Source Port:	49720
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.13549714174032816766 06/02/23-03:18:29.201957
SID:	2816766
Source Port:	49714
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.13549721174032816766 06/02/23-03:19:06.902900
SID:	2816766
Source Port:	49721
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949702174032816766 06/02/23-03:17:29.974643
SID:	2816766
Source Port:	49702
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.13549715174032816766 06/02/23-03:18:33.818642
SID:	2816766
Source Port:	49715
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.13549704174032816766 06/02/23-03:17:39.703803
SID:	2816766
Source Port:	49704
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.1354970517403281676 6 06/02/23-03:17:44.449297
SID:	2816766
Source Port:	49705
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.129.187.220	
Timestamp:	192.168.2.73.129.187.2204969917403281676 6 06/02/23-03:17:14.925523
SID:	2816766
Source Port:	49699
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.1354971617403281676 6 06/02/23-03:18:39.059373
SID:	2816766
Source Port:	49716
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949719174032816766 06/02/23-03:18:54.982902
SID:	2816766
Source Port:	49719
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.129.187.220	
Timestamp:	192.168.2.73.129.187.2204970017403281676 6 06/02/23-03:17:19.627500
SID:	2816766
Source Port:	49700
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.1354972317403281676 6 06/02/23-03:19:17.220052
SID:	2816766
Source Port:	49723
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949713174032816718 06/02/23-03:18:24.437024
SID:	2816718
Source Port:	49713
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.1354970817403281676 6 06/02/23-03:17:59.387763
SID:	2816766
Source Port:	49708

Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949718174032816766 06/02/23-03:18:49.091071
SID:	2816766
Source Port:	49718
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949717174032816766 06/02/23-03:18:43.892441
SID:	2816766
Source Port:	49717
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.1354970717403281676 6 06/02/23-03:17:54.419991
SID:	2816766
Source Port:	49707
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949706174032816766 06/02/23-03:17:49.649672
SID:	2816766
Source Port:	49706
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.7 - Destination IP: 3.22.15.135	
Timestamp:	192.168.2.73.22.15.1354970117403281671 8 06/02/23-03:17:24.631045
SID:	2816718
Source Port:	49701
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 3.131.147.49	
Timestamp:	192.168.2.73.131.147.4949703174032816766 06/02/23-03:17:34.772716
SID:	2816766
Source Port:	49703
Destination Port:	17403
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

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

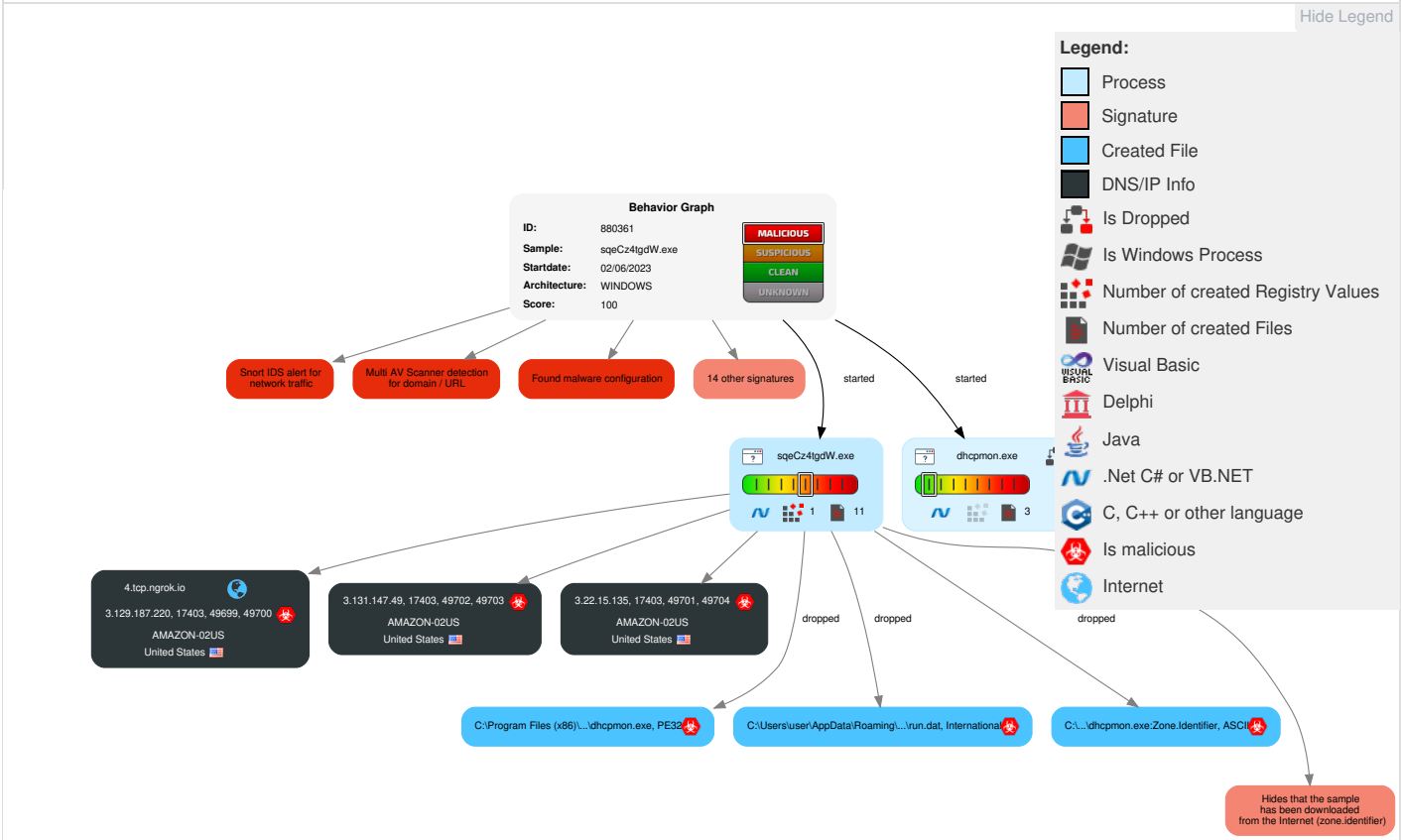
Yara detected Nanocore RAT

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	2 1 Input Capture	1 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 1 Software Packing	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

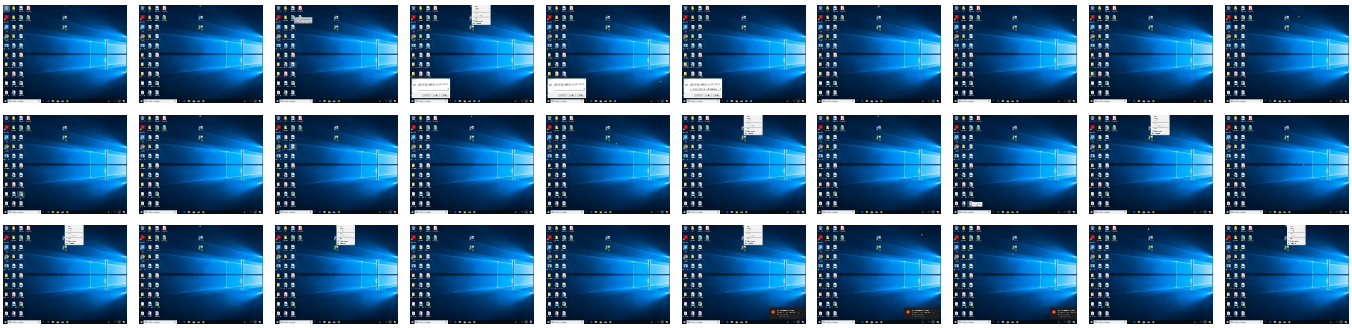
Behavior Graph



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
sqeCz4tgdW.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
sqeCz4tgdW.exe	92%	Virustotal		Browse
sqeCz4tgdW.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
sqeCz4tgdW.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	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
4.tcp.ngrok.io	21%	Virustotal		Browse

URLs

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

Domains and IPs

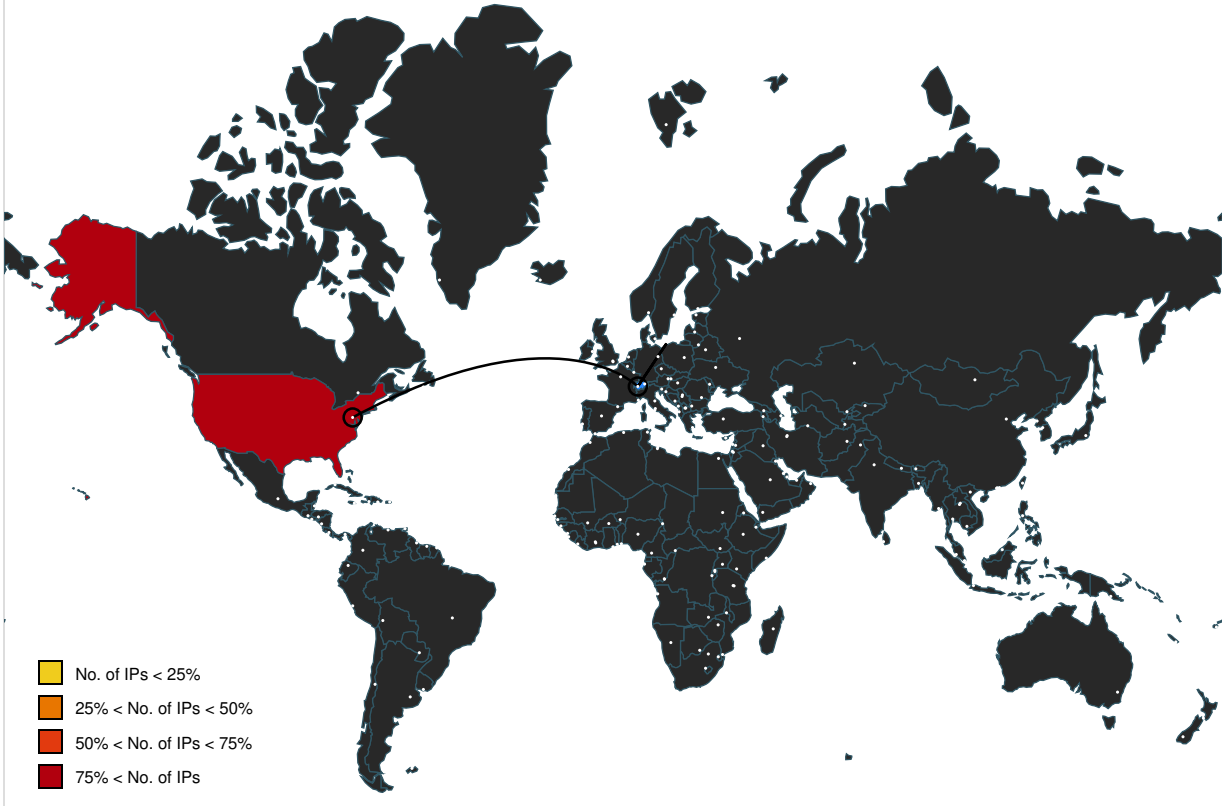
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
4.tcp.ngrok.io	3.129.187.220	true	true	• 21%, Virustotal, Browse	unknown

Contacted URLs

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

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.131.147.49	unknown	United States		16509	AMAZON-02US	true
3.129.187.220	4.tcp.ngrok.io	United States		16509	AMAZON-02US	true
3.22.15.135	unknown	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	880361
Start date and time:	2023-06-02 03:16:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
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:	5
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:	sqeCz4tgdW.exe
Original Sample Name:	0cea4eaf614191a2cf51abd70a672ed9.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@2/4@25/3
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target sqeCz4tgdW.exe, PID 7000 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.

Simulations

Behavior and APIs

Time	Type	Description
03:17:13	API Interceptor	875x Sleep call for process: sqeCz4tgdW.exe modified
03:17:17	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\sqeCz4tgdW.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.446808234153199
Encrypted:	false
SSDEEP:	6144:gLV6Bta6dtJmakIM5RlWUu5LYkO0TrWSo:gLV6BtpmkeIM5LYkO0TK9
MD5:	0CEA4EAF614191A2CF51ABD70A672ED9
SHA1:	1F5259A6EEEF5C641B324570F311BC8C86F32DC1
SHA-256:	597475447158DD0612E5584C51A515CABB3EAC9BD01681836318614CDA4878D0
SHA-512:	6CFE9F34EA558AD88084ADABB7DC049AD70A9F7418D05A0CA966A319A6CC55A87584B686787C6413797C39E3678BDE206FF59379D0F1CAE476F3272C02BE247 8
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ..p]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...p]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....- (&s8....-&&s9....,$&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\sqeCz4tgdW.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:	false
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\sqeCz4tgdW.exe
File Type:	International EBCDIC text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:y8+t:G
MD5:	73774CC6596C584012DF7F49C950AA18
SHA1:	5E8BE4474D2002A3EA53C37EB702463F1A35FD90
SHA-256:	37CD8E5FF28A70B4AE1FB96AEB1195B18DC9609EB73C58847F78E95281954C52
SHA-512:	BDF84B8CF190C3729B9B1829CEA5B6455E514CDFFF730ADB630543C58CC558E6AEFEB8200BFC11A35D82E98ABFC3E1923B42F97439FFBC8A8A6BAC0A32FEBCCD
Malicious:	**true**
Reputation:	low
Preview:	..Z.Rc.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.446808234153199
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:	sqeCz4tgdW.exe
File size:	207360

MD5:	0cea4eaf614191a2cf51abd70a672ed9
SHA1:	1f5259a6eeef5c641b324570f311bc8c86f32dc1
SHA256:	597475447158dd0612e5584c51a515cabb3eac9bd01681836318614cda4878d0
SHA512:	6cfe9f34ea558ad88084adabb7dc049ad70a9f7418d05a0ca966a319a6cc55a87584b686787c6413797c39e3678bde206ff59379d0f1cae476f3272c02be2478
SSDEEP:	6144:gLV6Bta6dtJmakIM5RlWUu5LYkO0TrWSo:gLV6BtpmkelM5LYkO0TK9
TLSH:	1514BF5677E94A2FE2DE86B9602251128379C2E3E8C3F7DE28D454F78B267E406071D3
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....'.T.....................`.......... ....@.. ....

File Icon

Icon Hash:	90cececece8e8eb0

Static PE Info

General

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

Entrypoint Preview

Instruction
jmp dword ptr [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

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

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	0.5945038377192983	data	6.5980557661789465	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15d70	0x15e00	False	0.9993303571428571	data	7.997699178073433	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x15d18	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

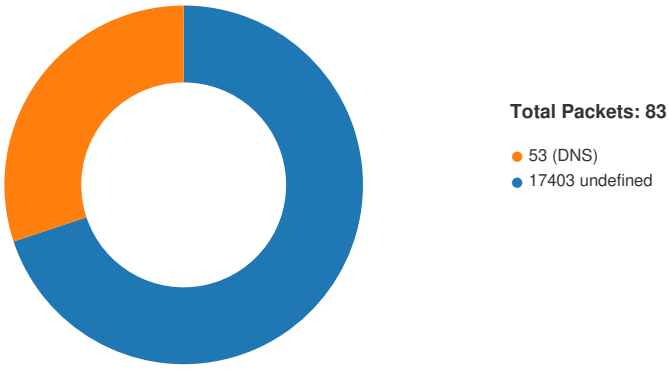
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.73.131.147.4949711174032816766 06/02/23-03:18:14.807235	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	17403	192.168.2.7	3.131.147.49
192.168.2.73.22.15.135497011174032816766 06/02/23-03:17:24.631045	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	17403	192.168.2.7	3.22.15.135
192.168.2.73.22.15.135497121174032816766 06/02/23-03:18:19.558845	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	17403	192.168.2.7	3.22.15.135
192.168.2.73.131.147.4949722174032816766 06/02/23-03:19:11.880129	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	17403	192.168.2.7	3.131.147.49
192.168.2.73.131.147.4949713174032816766 06/02/23-03:18:24.437024	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	17403	192.168.2.7	3.131.147.49
192.168.2.73.22.15.135497101174032816766 06/02/23-03:18:10.096340	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	17403	192.168.2.7	3.22.15.135
192.168.2.73.131.147.4949720174032816766 06/02/23-03:19:01.687305	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	17403	192.168.2.7	3.131.147.49
192.168.2.73.22.15.135497141174032816766 06/02/23-03:18:29.201957	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	17403	192.168.2.7	3.22.15.135
192.168.2.73.22.15.135497211174032816766 06/02/23-03:19:06.902900	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49721	17403	192.168.2.7	3.22.15.135
192.168.2.73.131.147.4949702174032816766 06/02/23-03:17:29.974643	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	17403	192.168.2.7	3.131.147.49
192.168.2.73.22.15.135497151174032816766 06/02/23-03:18:33.818642	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	17403	192.168.2.7	3.22.15.135
192.168.2.73.22.15.135497041174032816766 06/02/23-03:17:39.703803	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	17403	192.168.2.7	3.22.15.135
192.168.2.73.22.15.135497051174032816766 06/02/23-03:17:44.449297	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	17403	192.168.2.7	3.22.15.135
192.168.2.73.129.187.2204969174032816766 06/02/23-03:17:14.925523	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49699	17403	192.168.2.7	3.129.187.220
192.168.2.73.22.15.135497161174032816766 06/02/23-03:18:39.059373	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	17403	192.168.2.7	3.22.15.135
192.168.2.73.131.147.4949719174032816766 06/02/23-03:18:54.982902	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	17403	192.168.2.7	3.131.147.49
192.168.2.73.129.187.2204970174032816766 06/02/23-03:17:19.627500	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49700	17403	192.168.2.7	3.129.187.220
192.168.2.73.22.15.135497231174032816766 06/02/23-03:19:17.220052	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	17403	192.168.2.7	3.22.15.135

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.73.131.147.4949713174032816718 06/02/23-03:18:24.437024	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49713	17403	192.168.2.7	3.131.147.49
192.168.2.73.22.15.13549708174032816766 06/02/23-03:17:59.387763	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	17403	192.168.2.7	3.22.15.135
192.168.2.73.131.147.4949718174032816766 06/02/23-03:18:49.091071	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	17403	192.168.2.7	3.131.147.49
192.168.2.73.131.147.4949717174032816766 06/02/23-03:18:43.892441	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	17403	192.168.2.7	3.131.147.49
192.168.2.73.22.15.13549707174032816766 06/02/23-03:17:54.419991	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	17403	192.168.2.7	3.22.15.135
192.168.2.73.131.147.4949706174032816766 06/02/23-03:17:49.649672	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	17403	192.168.2.7	3.131.147.49
192.168.2.73.22.15.13549701174032816718 06/02/23-03:17:24.631045	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49701	17403	192.168.2.7	3.22.15.135
192.168.2.73.131.147.4949703174032816766 06/02/23-03:17:34.772716	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	17403	192.168.2.7	3.131.147.49

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:17:14.248718977 CEST	49699	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:14.404376984 CEST	17403	49699	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:14.404645920 CEST	49699	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:14.458405018 CEST	49699	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:14.613961935 CEST	17403	49699	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:14.614321947 CEST	49699	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:14.769804955 CEST	17403	49699	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:14.769936085 CEST	49699	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:14.925280094 CEST	17403	49699	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:14.925523043 CEST	49699	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:14.948740005 CEST	17403	49699	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:14.955879927 CEST	49699	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:19.005378008 CEST	49700	17403	192.168.2.7	3.129.187.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:17:19.160744905 CEST	17403	49700	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:19.160980940 CEST	49700	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:19.161511898 CEST	49700	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:19.316651106 CEST	17403	49700	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:19.316771030 CEST	49700	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:19.472047091 CEST	17403	49700	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:19.472188950 CEST	49700	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:19.627413988 CEST	17403	49700	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:19.627500057 CEST	49700	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:19.665241957 CEST	17403	49700	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:19.665477991 CEST	49700	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:19.782645941 CEST	17403	49700	3.129.187.220	192.168.2.7
Jun 2, 2023 03:17:19.782721043 CEST	49700	17403	192.168.2.7	3.129.187.220
Jun 2, 2023 03:17:23.903742075 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.058501959 CEST	17403	49701	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:24.058590889 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.059762001 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.214550972 CEST	17403	49701	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:24.214859009 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.369662046 CEST	17403	49701	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:24.382611036 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.537458897 CEST	17403	49701	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:24.538283110 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.628906012 CEST	17403	49701	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:24.631045103 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.631191015 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.693058014 CEST	17403	49701	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:24.694983006 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:24.786062002 CEST	17403	49701	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:24.786199093 CEST	49701	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:29.454476118 CEST	49702	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:29.609735012 CEST	17403	49702	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:29.609920025 CEST	49702	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:29.663494110 CEST	49702	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:29.818592072 CEST	17403	49702	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:29.818792105 CEST	49702	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:29.974524021 CEST	17403	49702	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:29.974642992 CEST	49702	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:30.101577997 CEST	17403	49702	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:30.101851940 CEST	49702	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:30.129663944 CEST	17403	49702	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:30.129792929 CEST	49702	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:34.145782948 CEST	49703	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:34.301250935 CEST	17403	49703	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:34.301405907 CEST	49703	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:34.302206039 CEST	49703	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:34.457386017 CEST	17403	49703	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:34.457461119 CEST	49703	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:34.612817049 CEST	17403	49703	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:34.616580009 CEST	49703	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:34.772546053 CEST	17403	49703	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:34.772716045 CEST	49703	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:34.797590017 CEST	17403	49703	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:34.799402952 CEST	49703	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:39.074366093 CEST	49704	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:39.229404926 CEST	17403	49704	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:39.229753017 CEST	49704	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:39.230129004 CEST	49704	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:39.384891033 CEST	17403	49704	3.22.15.135	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:17:39.389611959 CEST	49704	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:39.544677973 CEST	17403	49704	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:39.548490047 CEST	49704	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:39.703592062 CEST	17403	49704	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:39.703803062 CEST	49704	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:39.723170042 CEST	17403	49704	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:39.723527908 CEST	49704	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:43.786714077 CEST	49705	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:43.944698095 CEST	17403	49705	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:43.944829941 CEST	49705	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:43.984668016 CEST	49705	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:44.139517069 CEST	17403	49705	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:44.139671087 CEST	49705	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:44.294341087 CEST	17403	49705	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:44.294497013 CEST	49705	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:44.449165106 CEST	17403	49705	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:44.449296951 CEST	49705	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:44.467979908 CEST	17403	49705	3.22.15.135	192.168.2.7
Jun 2, 2023 03:17:44.468321085 CEST	49705	17403	192.168.2.7	3.22.15.135
Jun 2, 2023 03:17:49.026027918 CEST	49706	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:49.181377888 CEST	17403	49706	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:49.182033062 CEST	49706	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:49.182518959 CEST	49706	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:49.337843895 CEST	17403	49706	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:49.338016033 CEST	49706	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:49.493340015 CEST	17403	49706	3.131.147.49	192.168.2.7
Jun 2, 2023 03:17:49.493536949 CEST	49706	17403	192.168.2.7	3.131.147.49
Jun 2, 2023 03:17:49.649389029 CEST	17403	49706	3.131.147.49	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:17:14.207670927 CEST	60326	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:14.233273029 CEST	53	60326	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:18.982705116 CEST	50835	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:19.004167080 CEST	53	50835	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:23.866841078 CEST	50505	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:23.902790070 CEST	53	50505	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:29.400700092 CEST	61178	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:29.446557045 CEST	53	61178	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:34.123019934 CEST	63926	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:34.143059015 CEST	53	63926	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:39.044580936 CEST	53336	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:39.071871996 CEST	53	53336	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:43.756937981 CEST	51007	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:43.785307884 CEST	53	51007	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:48.994874954 CEST	50513	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:49.023816109 CEST	53	50513	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:53.718583107 CEST	60765	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:53.742288113 CEST	53	60765	8.8.8.8	192.168.2.7
Jun 2, 2023 03:17:58.735143900 CEST	58283	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:17:58.765738010 CEST	53	58283	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:04.513411999 CEST	50024	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:04.542355061 CEST	53	50024	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:09.343749046 CEST	49516	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:09.367266893 CEST	53	49516	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:14.124124050 CEST	62679	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:14.160327911 CEST	53	62679	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:18.908082962 CEST	61392	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:18:18.937267065 CEST	53	61392	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:23.725902081 CEST	52104	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:23.753962994 CEST	53	52104	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:28.549869061 CEST	65356	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:28.578433037 CEST	53	65356	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:33.305336952 CEST	59006	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:33.334503889 CEST	53	59006	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:38.403458118 CEST	51526	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:38.437822104 CEST	53	51526	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:43.240406990 CEST	51139	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:43.265762091 CEST	53	51139	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:48.363512993 CEST	58784	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:48.391935110 CEST	53	58784	8.8.8.8	192.168.2.7
Jun 2, 2023 03:18:54.312196970 CEST	57970	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:18:54.332453012 CEST	53	57970	8.8.8.8	192.168.2.7
Jun 2, 2023 03:19:01.031968117 CEST	64608	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:19:01.060734034 CEST	53	64608	8.8.8.8	192.168.2.7
Jun 2, 2023 03:19:06.258625031 CEST	58746	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:19:06.279195070 CEST	53	58746	8.8.8.8	192.168.2.7
Jun 2, 2023 03:19:11.240745068 CEST	62433	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:19:11.255553961 CEST	53	62433	8.8.8.8	192.168.2.7
Jun 2, 2023 03:19:16.326858997 CEST	61248	53	192.168.2.7	8.8.8.8
Jun 2, 2023 03:19:16.356242895 CEST	53	61248	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 2, 2023 03:17:14.207670927 CEST	192.168.2.7	8.8.8.8	0x8d3d	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:18.982705116 CEST	192.168.2.7	8.8.8.8	0xa613	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:23.866841078 CEST	192.168.2.7	8.8.8.8	0x40e	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:29.400700092 CEST	192.168.2.7	8.8.8.8	0x2ac3	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:34.123019934 CEST	192.168.2.7	8.8.8.8	0xb43	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:39.044580936 CEST	192.168.2.7	8.8.8.8	0x3a6e	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:43.756937981 CEST	192.168.2.7	8.8.8.8	0xcceb	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:48.994874954 CEST	192.168.2.7	8.8.8.8	0xf38a	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:53.718583107 CEST	192.168.2.7	8.8.8.8	0x1006	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:58.735143900 CEST	192.168.2.7	8.8.8.8	0x5260	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:04.513411999 CEST	192.168.2.7	8.8.8.8	0x7ec0	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:09.343749046 CEST	192.168.2.7	8.8.8.8	0xe177	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:14.124124050 CEST	192.168.2.7	8.8.8.8	0x98c9	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:18.908082962 CEST	192.168.2.7	8.8.8.8	0x621c	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:23.725902081 CEST	192.168.2.7	8.8.8.8	0x863e	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:28.549869061 CEST	192.168.2.7	8.8.8.8	0xb18f	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:33.305336952 CEST	192.168.2.7	8.8.8.8	0xf9d4	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:38.403458118 CEST	192.168.2.7	8.8.8.8	0xc2f6	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:43.240406990 CEST	192.168.2.7	8.8.8.8	0x470f	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 2, 2023 03:18:48.363512993 CEST	192.168.2.7	8.8.8.8	0x2450	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:54.312196970 CEST	192.168.2.7	8.8.8.8	0x1efc	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:01.031968117 CEST	192.168.2.7	8.8.8.8	0x26c1	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:06.258625031 CEST	192.168.2.7	8.8.8.8	0xd77d	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:11.240745068 CEST	192.168.2.7	8.8.8.8	0x6db7	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:16.326858997 CEST	192.168.2.7	8.8.8.8	0xf75f	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)	false

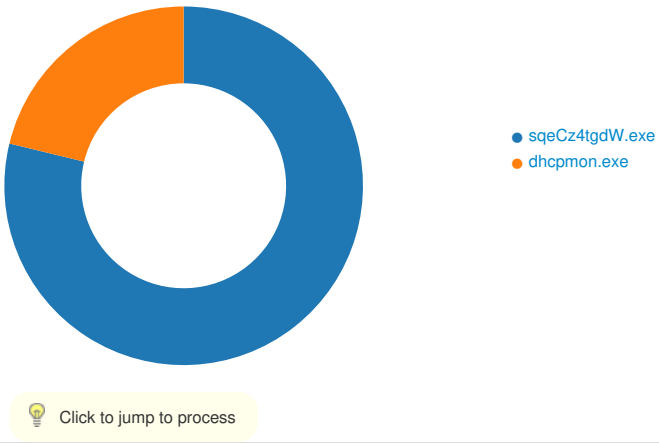
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 03:17:14.233273029 CEST	8.8.8.8	192.168.2.7	0x8d3d	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:19.004167080 CEST	8.8.8.8	192.168.2.7	0xa613	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:23.902790070 CEST	8.8.8.8	192.168.2.7	0x40e	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:29.446557045 CEST	8.8.8.8	192.168.2.7	0x2ac3	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:34.143059015 CEST	8.8.8.8	192.168.2.7	0xb43	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:39.071871996 CEST	8.8.8.8	192.168.2.7	0x3a6e	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:43.785307884 CEST	8.8.8.8	192.168.2.7	0xcceb	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:49.023816109 CEST	8.8.8.8	192.168.2.7	0xf38a	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:53.742288113 CEST	8.8.8.8	192.168.2.7	0x1006	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:17:58.765738010 CEST	8.8.8.8	192.168.2.7	0x5260	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:04.542355061 CEST	8.8.8.8	192.168.2.7	0x7ec0	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:09.367266893 CEST	8.8.8.8	192.168.2.7	0xe177	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:14.160327911 CEST	8.8.8.8	192.168.2.7	0x98c9	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:18.937267065 CEST	8.8.8.8	192.168.2.7	0x621c	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:23.753962994 CEST	8.8.8.8	192.168.2.7	0x863e	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:28.578433037 CEST	8.8.8.8	192.168.2.7	0xb18f	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:33.334503889 CEST	8.8.8.8	192.168.2.7	0xf9d4	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:38.437822104 CEST	8.8.8.8	192.168.2.7	0xc2f6	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:43.265762091 CEST	8.8.8.8	192.168.2.7	0x470f	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 03:18:48.391935110 CEST	8.8.8.8	192.168.2.7	0x2450	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:18:54.332453012 CEST	8.8.8.8	192.168.2.7	0x1efc	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:01.060734034 CEST	8.8.8.8	192.168.2.7	0x26c1	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:06.279195070 CEST	8.8.8.8	192.168.2.7	0xd77d	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:11.255553961 CEST	8.8.8.8	192.168.2.7	0x6db7	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:19:16.356242895 CEST	8.8.8.8	192.168.2.7	0xf75f	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: sqeCz4tgdW.exe PID: 7000, Parent PID: 3320

General

Target ID:	0
Start time:	03:17:11
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\sqeCz4tgdW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\sqeCz4tgdW.exe
Imagebase:	0xba0000
File size:	207360 bytes
MD5 hash:	0CEA4EAF614191A2CF51ABD70A672ED9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.613140650.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.336434813.0000000000BA2000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.336434813.0000000000BA2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.336434813.0000000000BA2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000000.336434813.0000000000BA2000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.613534042.0000000005AD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.613534042.0000000005AD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.613534042.0000000005AD0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.613534042.0000000005AD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.613534042.0000000005AD0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.608684024.0000000003201000.00000004.00000800.00020000.00000000.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	6CAB60AC	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	6CAB60AC	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	54B0D15	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	54B0E0F	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	54B0D15	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	54B1094	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	54B1094	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	54B0D15	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	54B0D15	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	6CAB60AC	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	6CAB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\sqeCz4tgdW.exe:Zone.Identifier	success or wait	1	54B1265	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	7f fd 5a fd 52 63 fd 48	ZRcH	success or wait	1	54B0FC7	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 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	54B1094	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	54B1094	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	6CAE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CAE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CAE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CB8BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CB8BF06	unknown
C:\Users\user\Desktop\sqeCz4tgdW.exe	unknown	4096	success or wait	1	6CB8BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\sqeCz4tgdW.exe	unknown	512	success or wait	1	6CB8BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CAE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6CAE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	54B0FC7	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	54B1186	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **3568**, Parent PID: **3320**

General

Target ID:	1
Start time:	03:17:26
Start date:	02/06/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x510000
File size:	207360 bytes
MD5 hash:	0CEA4EAF614191A2CF51ABD70A672ED9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.385393945.0000000003AF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.385393945.0000000003AF1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.385393945.0000000003AF1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.385333810.0000000002AF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.385333810.0000000002AF1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.385333810.0000000002AF1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 97%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CAB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CAB60AC	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	6CAA34A7	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	6CD8A33A	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	6CAE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CAE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CAE8738	ReadFile

Disassembly

No disassembly