ID: 880358
Sample Name: mfpmp.exe
Cookbook: default.jbs
Time: 03:13:14
Date: 02/06/2023
Version: 37.1.0 Beryl

Table of Contents

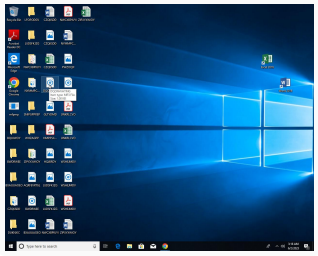
Windows Analysis Report

mfpmp.exe

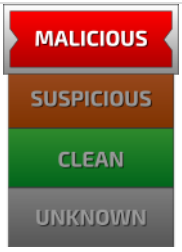
Overview

General Information

Sample Name:	mfpmp.exe
Analysis ID:	880358
MD5:	475b4814a0b6…
SHA1:	d9cb6110591e…
SHA256:	10feb93ebdb8d..
Tags:	exe NanoCore
Infos:	



Detection



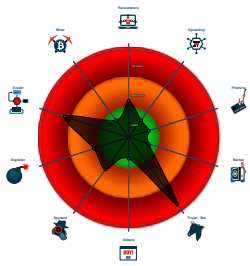
Nanocore

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
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- mfpmp.exe (PID: 6504 cmdline: C:\Users\user\Desktop\mfpmp.exe MD5: 475B4814A0B6114C76EA55C7447B6108)
- **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": "6f656d69-7475-8507-1300-000c0a4c",
  "Group": "Default",
  "Domain1": "dinowar.anondns.net",
  "Domain2": "dinowar.dynv6.net",
  "Port": 21942,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "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": 4997,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "1a000100",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "f4ff9f00",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
mfpmp.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
mfpmp.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
mfpmp.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
mfpmp.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
mfpmp.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
00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0xff8d:$x1: NanoCore.ClientPluginHost 0xffca:$x2: IClientNetworkHost 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfcf5:$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
00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0xff8d:$a1: NanoCore.ClientPluginHost 0xff4d:$a2: NanoCore.ClientPlugin 0x11ea6:$b1: get_BuilderSettings 0xfda9:$b2: ClientLoaderForm.resources 0x115c6:$b3: PluginCommand 0xff7e:$b4: IClientAppHost 0x1a3fe:$b5: GetBlockHash 0x124fe:$b6: AddHostEntry 0x161f1:$b7: LogClientException 0x1246b:$b8: PipeExists 0xffb7:$b9: IClientLoggingHost
00000000.00000002.657080001.0000000002991000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0x11591:$a1: NanoCore.ClientPluginHost 0x16bde:$a1: NanoCore.ClientPluginHost 0x11554:$a2: NanoCore.ClientPlugin 0x16c28:$a2: NanoCore.ClientPlugin 0x11928:$b1: get_BuilderSettings 0x115df:$b4: IClientAppHost 0x11999:$b6: AddHostEntry 0x11a08:$b7: LogClientException 0x1197d:$b8: PipeExists 0x115cc:$b9: IClientLoggingHost 0x16bf8:$b9: IClientLoggingHost
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.mfpmp.exe.29a171c.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x40c2:$x1: NanoCore.ClientPluginHost
0.2.mfpmp.exe.29a171c.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x40c2:$x2: NanoCore.ClientPluginHost • 0x41a0:$s4: PipeCreated • 0x40dc:$s5: IClientLoggingHost
0.2.mfpmp.exe.29a171c.1.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x410c:$x2: NanoCore.ClientPlugin • 0x40c2:$x3: NanoCore.ClientPluginHost • 0x4122:$i3: IClientNetwork • 0x40dc:$i6: IClientLoggingHost • 0x3e5b:$s1: ClientPlugin • 0x4115:$s1: ClientPlugin
0.2.mfpmp.exe.29a171c.1.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x40c2:$a1: NanoCore.ClientPluginHost • 0x410c:$a2: NanoCore.ClientPlugin • 0x40dc:$b9: IClientLoggingHost
0.2.mfpmp.exe.3a019a0.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 51 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: 192.168.2.5 - Destination IP: 213.152.161.40 −

Timestamp:	192.168.2.5213.152.161.404972621942281676 6/02/23-03:15:58.229871
SID:	2816766
Source Port:	49726
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40 −

Timestamp:	192.168.2.5213.152.161.404972521942281676 6/02/23-03:15:46.918356
SID:	2816766
Source Port:	49725
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40 −

Timestamp:	192.168.2.5213.152.161.404972721942281676 6/02/23-03:16:05.832874
SID:	2816766

Source Port:	49727
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	−
Timestamp:	192.168.2.5213.152.161.404971421942281676 6/02/23-03:14:23.945597
SID:	2816766
Source Port:	49714
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	−
Timestamp:	192.168.2.5213.152.161.404971621942281676 6/02/23-03:14:38.958735
SID:	2816766
Source Port:	49716
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	−
Timestamp:	192.168.2.5213.152.161.404972421942281676 6/02/23-03:15:41.133556
SID:	2816766
Source Port:	49724
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	−
Timestamp:	192.168.2.5213.152.161.404972821942281676 6/02/23-03:16:14.874731
SID:	2816766
Source Port:	49728
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	−
Timestamp:	192.168.2.5213.152.161.404971321942281676 6/02/23-03:14:17.578597
SID:	2816766
Source Port:	49713
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	−
Timestamp:	192.168.2.5213.152.161.404971721942281676 6/02/23-03:14:46.659916
SID:	2816766
Source Port:	49717
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	−
Timestamp:	192.168.2.5213.152.161.404971521942281676 6/02/23-03:14:32.676847
SID:	2816766
Source Port:	49715
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049723219422025019 06/02/23-03:15:30.905805
SID:	2025019
Source Port:	49723
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049722219422816766 06/02/23-03:15:18.909197
SID:	2816766
Source Port:	49722
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049713219422025019 06/02/23-03:14:16.340330
SID:	2025019
Source Port:	49713
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049714219422025019 06/02/23-03:14:22.701480
SID:	2025019
Source Port:	49714
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049724219422025019 06/02/23-03:15:38.625540
SID:	2025019
Source Port:	49724
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049725219422025019 06/02/23-03:15:46.516736
SID:	2025019
Source Port:	49725
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049721219422816766 06/02/23-03:15:11.972977
SID:	2816766
Source Port:	49721
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049723219422816766 06/02/23-03:15:32.602475
SID:	2816766
Source Port:	49723

Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049715219422025019 06/02/23-03:14:29.058470
SID:	2025019
Source Port:	49715
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049726219422025019 06/02/23-03:15:56.130210
SID:	2025019
Source Port:	49726
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049728219422025019 06/02/23-03:16:12.322829
SID:	2025019
Source Port:	49728
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049717219422025019 06/02/23-03:14:45.071339
SID:	2025019
Source Port:	49717
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049718219422025019 06/02/23-03:14:54.530247
SID:	2025019
Source Port:	49718
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 213.152.161.40 - Destination IP: 192.168.2.5	
Timestamp:	213.152.161.40192.168.2.521942497252841753 06/02/23-03:15:53.656106
SID:	2841753
Source Port:	21942
Destination Port:	49725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049716219422025019 06/02/23-03:14:38.559097
SID:	2025019
Source Port:	49716
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049727219422025019 06/02/23-03:16:05.006045
SID:	2025019
Source Port:	49727
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049719219422025019 06/02/23-03:15:01.548154
SID:	2025019
Source Port:	49719
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049722219422025019 06/02/23-03:15:17.333804
SID:	2025019
Source Port:	49722
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049721219422025019 06/02/23-03:15:10.736542
SID:	2025019
Source Port:	49721
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049718219422816766 06/02/23-03:14:55.770847
SID:	2816766
Source Port:	49718
Destination Port:	21942
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 213.152.161.40	
Timestamp:	192.168.2.5213.152.161.4049719219422816766 06/02/23-03:15:03.125668
SID:	2816766
Source Port:	49719
Destination Port:	21942
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

Yara detected Nanocore RAT

Machine Learning detection for sample

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

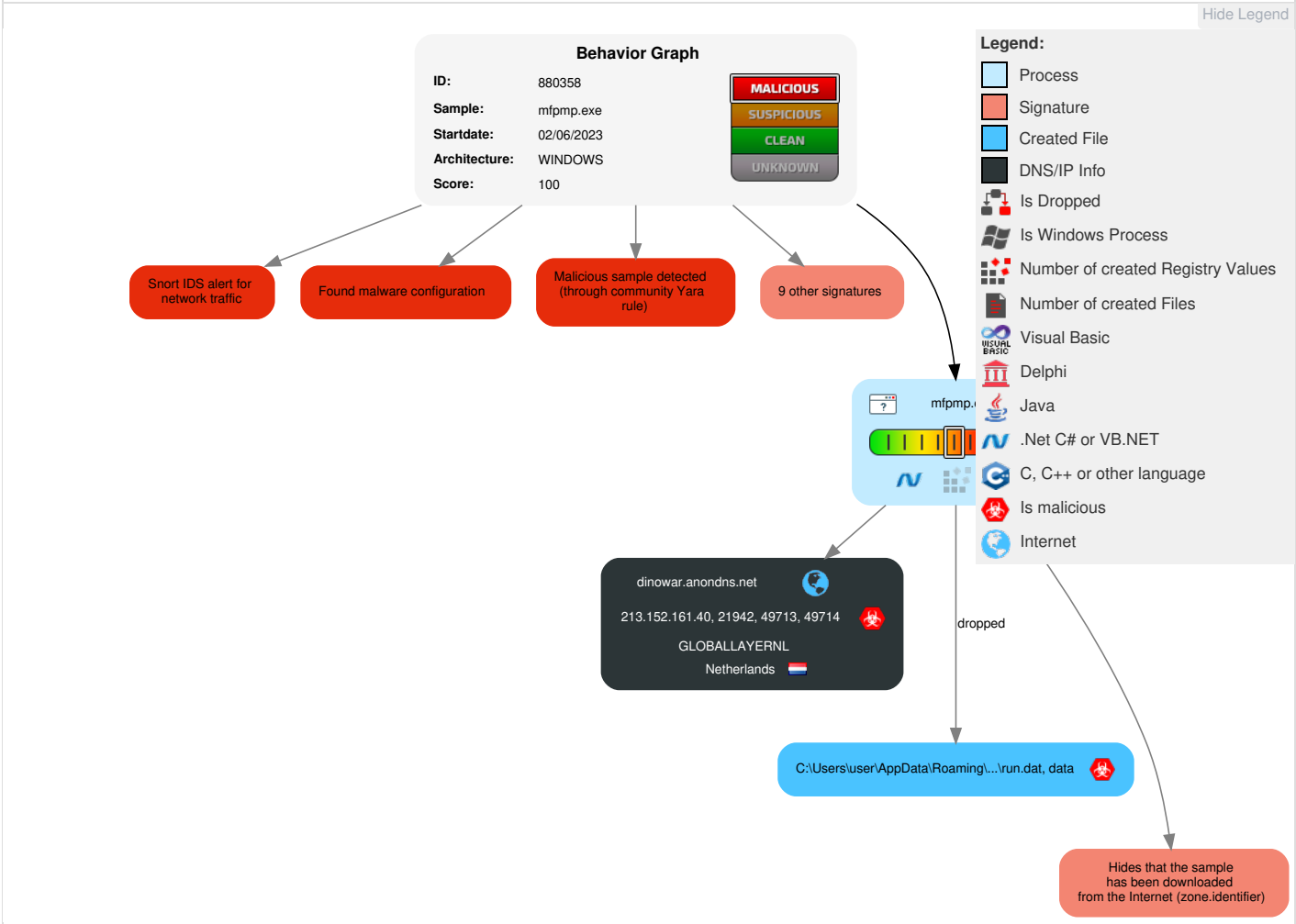
Yara detected Nanocore RAT

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	1 Access Token Manipulation	1 Masquerading	2 1 Input Capture	1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Process Injection	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	3 System Information Discovery	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	2 Obfuscated Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 1 Software Packing	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

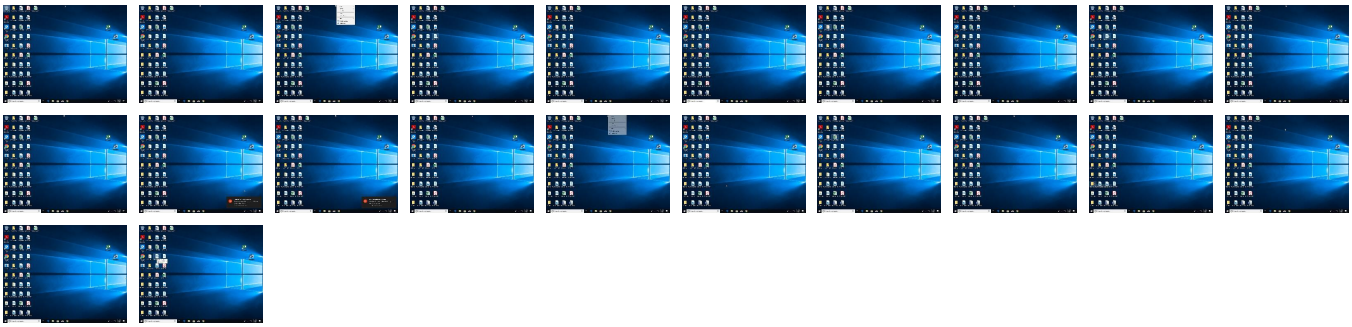
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
mfpmp.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
mfpmp.exe	88%	Virustotal		Browse
mfpmp.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
mfpmp.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dinowar.anondns.net	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
dinowar.dynv6.net	2%	Virustotal		Browse
dinowar.anondns.net	3%	Virustotal		Browse
dinowar.anondns.net	100%	Avira URL Cloud	malware	
dinowar.dynv6.net	100%	Avira URL Cloud	malware	

Domains and IPs

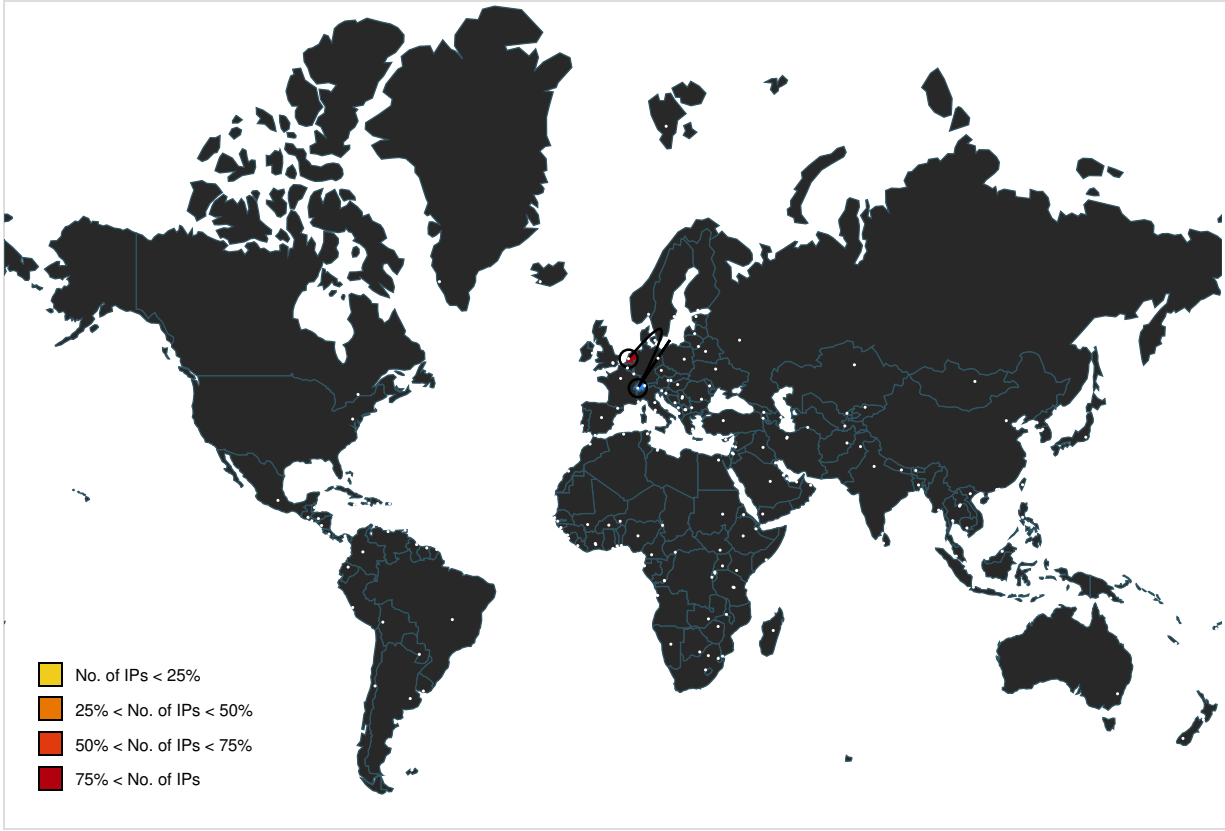
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dinowar.anondns.net	213.152.161.40	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
dinowar.anondns.net	true	• 3%, Virustotal, Browse • Avira URL Cloud: malware	unknown
dinowar.dynv6.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.152.161.40	dinowar.anondns.net	Netherlands		49453	GLOBALLAYERNL	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	880358
Start date and time:	2023-06-02 03:13:14 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
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:	4
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:	mfpmp.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/2@18/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report 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
03:14:14	API Interceptor	914x Sleep call for process: mfpmp.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\mfpmp.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	6.997351629001838
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcps0Oa706d+6zsThvr9ohWCsT9ZIWyq4B:X4LEnybgCF07hNgtr9oE/3oB
MD5:	EDB5F15385E111D1F43093F56149A3FB
SHA1:	D865A47A0997848D5D4005B857A3FD0027BCD3C6
SHA-256:	1995E579108E8EB3B6C00893E855E8204D1C36F150088736556B66BE445E7957

SHA-512:	C3C0ADA45BECD863F41369F766E719A6FDC7807096F17FAEFBA6466EBEE4830524046DAFB186E1DFB50B15B07F0877ECD3B4E5993B83E8D67FF5A68D4F2ACC FE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*.....S.Ty.K.&....q$.7....."....F... .N.k.C.X.D.^.....u.\...X.....s^.;...m/.,7X.. v"B..#.T.F L...h.....t 5.|Z

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

Process:	C:\Users\user\Desktop\mfpmp.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:V66pt:1
MD5:	C8A6A661D6743E259E659C36B4C72D17
SHA1:	1526F977C40AB1700E731F506D7FFB2BC440ED9E
SHA-256:	AD606B5A81C70DDA9F84813BAAAF04DE4605FCA79877D9B9F2C69316605A5C29
SHA-512:	15598B836EF25A356884598B374A5CDF286812B4DFB13A5D266F16AC60B8F36FC9114823A390B72AF44ACA63AC1CD9CE29EDC40F8E827B749708AD0620A6804
Malicious:	**true**
Reputation:	low
Preview:	.a..Rc.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.476662499761944
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:	mfpmp.exe
File size:	214528
MD5:	475b4814a0b6114c76ea55c7447b6108
SHA1:	d9cb6110591e7fb53a29ee7c8efd2c7132b3a426
SHA256:	10feb93ebdb8dd942d6b7a878d1ee3920584e89cdead6e34ae8292bfb1916116
SHA512:	cb822c8b67d1733a9d4779d1e35c737db6f4ad47d2ded10aacdcd7d85acf72e58eb71d2b8bbb90e9c271041efe87f5654ea661bd786d8376d6fc4b4717c82c9b
SSDEEP:	6144:ELV6Bta6dtJmakIM5zmMVrunW9jnHzmycg81x:ELV6Btpmk8msrunW9P+
TLSH:	B724CF167BA84A3FE2DE8AB9711211028379C2E398C3F3DE5CD495B74B267E50A071D7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....|..... .....@.. .....

File Icon

Icon Hash:	90cecececе8e8eb0

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

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	0x17860	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0.5945124040570176	data	6.59808650483268	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	0x17860	0x17a00	False	0.9965897817460317	data	7.997328427019175	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x17808	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

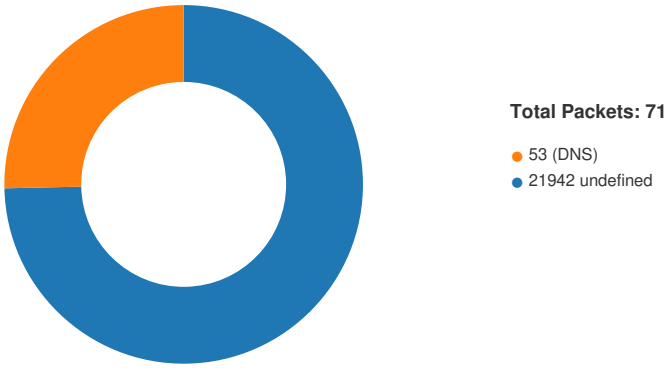
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5213.152.161.40497262194228167666/02/23-03:15:58.229871	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49726	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497252194228167666/02/23-03:15:46.918356	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49725	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497272194228167666/02/23-03:16:05.832874	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49727	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497142194228167666/02/23-03:14:23.945597	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497162194228167666/02/23-03:14:38.958735	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497242194228167666/02/23-03:15:41.133556	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49724	21942	192.168.2.5	213.152.161.40

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5213.152.161.40497282194228167666/02/23-03:16:14.874731	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49728	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497132194228167666/02/23-03:14:17.578597	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497172194228167666/02/23-03:14:46.659916	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497152194228167666/02/23-03:14:32.676847	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497232194220250196/02/23-03:15:30.905805	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497222194228167666/02/23-03:15:18.909197	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497132194220250196/02/23-03:14:16.340330	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497142194220250196/02/23-03:14:22.701480	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497242194220250196/02/23-03:15:38.625540	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497252194220250196/02/23-03:15:46.516736	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497212194228167666/02/23-03:15:11.972977	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49721	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497232194228167666/02/23-03:15:32.602475	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497152194220250196/02/23-03:14:29.058470	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497262194220250196/02/23-03:15:56.130210	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497282194220250196/02/23-03:16:12.322829	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497172194220250196/02/23-03:14:45.071339	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.40497182194220250196/02/23-03:14:54.530247	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	21942	192.168.2.5	213.152.161.40
213.152.161.40192.168.2.521942497252841753 06/02/23-03:15:53.656106	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	21942	49725	213.152.161.40	192.168.2.5
192.168.2.5213.152.161.40497162194220250196/02/23-03:14:38.559097	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	21942	192.168.2.5	213.152.161.40

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5213.152.161.4 049727219422025019 06/02/23-03:16:05.006045	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.4 049719219422025019 06/02/23-03:15:01.548154	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.4 049722219422025019 06/02/23-03:15:17.333804	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.4 049721219422025019 06/02/23-03:15:10.736542	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.4 049718219422816766 06/02/23-03:14:55.770847	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	21942	192.168.2.5	213.152.161.40
192.168.2.5213.152.161.4 049719219422816766 06/02/23-03:15:03.125668	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	21942	192.168.2.5	213.152.161.40

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:14:15.897165060 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:16.291115046 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:16.292726994 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:16.340329885 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:16.740214109 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:16.741002083 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:17.182162046 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:17.182327032 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:17.577496052 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:17.578597069 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.023407936 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.023624897 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.153752089 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.452577114 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.452625036 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.452646971 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.452670097 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.452670097 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.452722073 CEST	21942	49713	213.152.161.40	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:14:18.452725887 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.452780008 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.452780008 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.452825069 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.453490019 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.453512907 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.453535080 CEST	21942	49713	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:18.453617096 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:18.453643084 CEST	49713	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:22.293716908 CEST	49714	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:22.689059019 CEST	21942	49714	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:22.689198971 CEST	49714	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:22.701479912 CEST	49714	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:23.106259108 CEST	21942	49714	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:23.107754946 CEST	49714	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:23.549438000 CEST	21942	49714	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:23.550512075 CEST	49714	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:23.945451975 CEST	21942	49714	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:23.945596933 CEST	49714	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:24.559926987 CEST	49714	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:28.666457891 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:29.057277918 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:29.057544947 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:29.058470011 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:29.456240892 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:29.456424952 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:30.233597994 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:30.636657953 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:30.636878014 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.069416046 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.073952913 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.500612974 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.500646114 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.500659943 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.500674009 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.500886917 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.501477003 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.501518965 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.501518965 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.501554012 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.501625061 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.501672983 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.501741886 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.501791000 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.892621040 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.892793894 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.892899036 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.892967939 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.893393040 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.893415928 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.893439054 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.893467903 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.893497944 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.893512964 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:31.894252062 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:31.894345045 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.200197935 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.284379959 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.284544945 CEST	49715	21942	192.168.2.5	213.152.161.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:14:32.284564972 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.284594059 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.284624100 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.284672976 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.284677982 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.284704924 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.284723997 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.284744978 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.285245895 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.285310030 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.645306110 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.645418882 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.675637007 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.675745964 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.676757097 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.676791906 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.676811934 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.676831961 CEST	21942	49715	213.152.161.40	192.168.2.5
Jun 2, 2023 03:14:32.676846981 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.676846981 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.676883936 CEST	49715	21942	192.168.2.5	213.152.161.40
Jun 2, 2023 03:14:32.676893950 CEST	49715	21942	192.168.2.5	213.152.161.40

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:14:15.853120089 CEST	49177	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:14:15.885448933 CEST	53	49177	8.8.8.8	192.168.2.5
Jun 2, 2023 03:14:22.231913090 CEST	49724	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:14:22.253011942 CEST	53	49724	8.8.8.8	192.168.2.5
Jun 2, 2023 03:14:28.631515026 CEST	61452	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:14:28.664314032 CEST	53	61452	8.8.8.8	192.168.2.5
Jun 2, 2023 03:14:37.110941887 CEST	65323	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:14:37.149499893 CEST	53	65323	8.8.8.8	192.168.2.5
Jun 2, 2023 03:14:44.644526005 CEST	51484	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:14:44.672653913 CEST	53	51484	8.8.8.8	192.168.2.5
Jun 2, 2023 03:14:51.091420889 CEST	63446	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:14:51.118262053 CEST	53	63446	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:01.121577978 CEST	56751	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:01.150638103 CEST	53	56751	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:09.295682907 CEST	60975	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:09.324079990 CEST	53	60975	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:16.925514936 CEST	59220	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:16.940361977 CEST	53	59220	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:23.323892117 CEST	55068	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:24.376849890 CEST	55068	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:25.449541092 CEST	55068	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:27.482081890 CEST	53	55068	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:37.110519886 CEST	56682	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:38.121855974 CEST	56682	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:38.144364119 CEST	53	56682	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:39.134860039 CEST	53	56682	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:46.034936905 CEST	58532	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:46.071866035 CEST	53	58532	8.8.8.8	192.168.2.5
Jun 2, 2023 03:15:52.640743017 CEST	62659	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:15:52.668926954 CEST	53	62659	8.8.8.8	192.168.2.5
Jun 2, 2023 03:16:03.578902960 CEST	58581	53	192.168.2.5	8.8.8.8
Jun 2, 2023 03:16:03.599817038 CEST	53	58581	8.8.8.8	192.168.2.5
Jun 2, 2023 03:16:11.905319929 CEST	56263	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 03:16:11.926800966 CEST	53	56263	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jun 2, 2023 03:15:39.135045052 CEST	192.168.2.5	8.8.8.8	d008	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 2, 2023 03:14:15.853120089 CEST	192.168.2.5	8.8.8.8	0x96b3	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:22.231913090 CEST	192.168.2.5	8.8.8.8	0x367a	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:28.631515026 CEST	192.168.2.5	8.8.8.8	0x1016	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:37.110941887 CEST	192.168.2.5	8.8.8.8	0x1c00	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:44.644526005 CEST	192.168.2.5	8.8.8.8	0xc195	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:51.091420889 CEST	192.168.2.5	8.8.8.8	0x997c	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:01.121577978 CEST	192.168.2.5	8.8.8.8	0xb8bf	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:09.295682907 CEST	192.168.2.5	8.8.8.8	0x9cdf	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:16.925514936 CEST	192.168.2.5	8.8.8.8	0x8754	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:23.323892117 CEST	192.168.2.5	8.8.8.8	0xd62c	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:24.376849890 CEST	192.168.2.5	8.8.8.8	0xd62c	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:25.449541092 CEST	192.168.2.5	8.8.8.8	0xd62c	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:37.110519886 CEST	192.168.2.5	8.8.8.8	0x89d3	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:38.121855974 CEST	192.168.2.5	8.8.8.8	0x89d3	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:46.034936905 CEST	192.168.2.5	8.8.8.8	0xf3b5	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:52.640743017 CEST	192.168.2.5	8.8.8.8	0xaee7	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:16:03.578902960 CEST	192.168.2.5	8.8.8.8	0x1577	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:16:11.905319929 CEST	192.168.2.5	8.8.8.8	0xf81a	Standard query (0)	dinowar.andns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 03:14:15.885448933 CEST	8.8.8.8	192.168.2.5	0x96b3	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:22.253011942 CEST	8.8.8.8	192.168.2.5	0x367a	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:28.664314032 CEST	8.8.8.8	192.168.2.5	0x1016	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:37.149499893 CEST	8.8.8.8	192.168.2.5	0x1c00	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:44.672653913 CEST	8.8.8.8	192.168.2.5	0xc195	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:14:51.118262053 CEST	8.8.8.8	192.168.2.5	0x997c	No error (0)	dinowar.andns.net		213.152.161.40	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 03:15:01.150638103 CEST	8.8.8.8	192.168.2.5	0xb8bf	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:09.324079990 CEST	8.8.8.8	192.168.2.5	0x9cdf	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:16.940361977 CEST	8.8.8.8	192.168.2.5	0x8754	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:27.482081890 CEST	8.8.8.8	192.168.2.5	0xd62c	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:38.144364119 CEST	8.8.8.8	192.168.2.5	0x89d3	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:39.134860039 CEST	8.8.8.8	192.168.2.5	0x89d3	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:46.071866035 CEST	8.8.8.8	192.168.2.5	0xf3b5	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:15:52.668926954 CEST	8.8.8.8	192.168.2.5	0xaee7	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:16:03.599817038 CEST	8.8.8.8	192.168.2.5	0x1577	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false
Jun 2, 2023 03:16:11.926800966 CEST	8.8.8.8	192.168.2.5	0xf81a	No error (0)	dinowar.andns.net		213.152.161.40	A (IP address)	IN (0x0001)	false

Statistics

No statistics

System Behavior

Analysis Process: mfpmp.exe PID: **6504**, Parent PID: **3324**

General

Target ID:	0
Start time:	03:14:13
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\mfpmp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\mfpmp.exe
Imagebase:	0x2d0000
File size:	214528 bytes
MD5 hash:	475B4814A0B6114C76EA55C7447B6108
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: 00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000000.390950299.00000000002D2000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.657080001.0000000002991000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.667317565.0000000004CC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.667317565.0000000004CC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.667317565.0000000004CC0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.667317565.0000000004CC0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.667774340.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.667774340.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.667774340.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.667774340.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.667674827.00000000051D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.667674827.00000000051D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.667674827.00000000051D0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.667674827.00000000051D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.667674827.00000000051D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.665497536.00000000039F2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.665497536.00000000039F2000.00000004.00000800.00020000.00000000.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	6BE760AC	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	6BE760AC	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	4B00D15	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	4B00E0F	CreateFileW
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	4B00D15	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4B00D15	CreateDirectoryW

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	6BE760AC	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	6BE760AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	12	4B00E0F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\mfpmp.exe:Zone.Identifier	success or wait	1	4B010B5	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	19 61 fd 1d 52 63 fd 48	aRcH	success or wait	1	4B00FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	248	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e 70 fd fd 0b fd fd fd 09 fd fd 53 fd 54 79 fd 4b fd 26 fd fd fd 0f 71 24 fd 37 fd fd fd fd 0b 22 fd 1d fd 1e 46 fd fd 17 20 0e 4e fd 6b fd 43 fd 58 fd 44 fd 5e 10 fd 12 fd fd 75 fd 5c fd fd d2 58 10 fd 7f 1d cd fd 7f fd 73 5e fd 3b fd 2e fd 6d 2f fd 2c 37 58 01 83 76 22 42 fd 7f 23 fd 54 1d 46 20 4c c3 fd fd 68 fd fd 8f fd fd 74 20 35 1d 7c 5a	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*STyK&q $7"F NkCXD^ u\Xs^;.m/,7Xv"B#TF Lht 5|Z	success or wait	12	4B00FC7	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	6BEA5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6BEA5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BEA8738	ReadFile
C:\Users\user\Desktop\mfpmp.exe	unknown	4096	success or wait	1	6BF4BF06	unknown
C:\Users\user\Desktop\mfpmp.exe	unknown	512	success or wait	1	6BF4BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BEA5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6BEA5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4B00FC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6BF4BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6BF4BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6BF4BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6BF4BF06	unknown

Disassembly

No disassembly