ID: 798399
Sample Name: HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
Cookbook: default.jbs
Time: 04:01:07
Date: 04/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

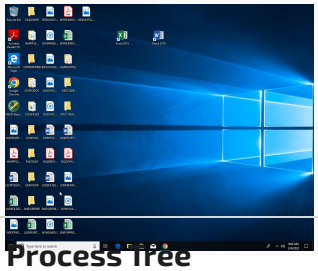
Windows Analysis Report

HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe

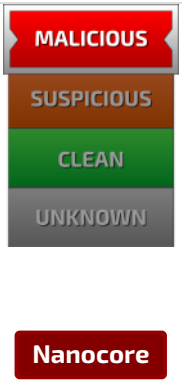
Overview

General Information

Sample Name:	HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
Analysis ID:	798399
MD5:	8c4f47a96a1f9…
SHA1:	4e7e9f7c7d630..
SHA256:	e1cfeeaabcfa9…
Tags:	exe NanoCore RAT
Infos:	



Detection

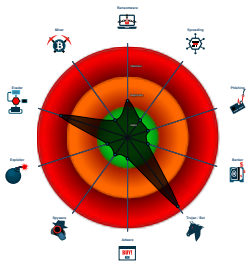


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe (PID: 4864 cmdline: C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe MD5: 8C4F47A96A1F9F58AB28A2353627C153)
  - HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe (PID: 5368 cmdline: C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe MD5: 8C4F47A96A1F9F58AB28A2353627C153)
- dhcpmon.exe (PID: 5240 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 8C4F47A96A1F9F58AB28A2353627C153)
  - dhcpmon.exe (PID: 5168 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 8C4F47A96A1F9F58AB28A2353627C153)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "b210040d-15e5-44d6-9102-34199926",
  "Group": "Default",
  "Domain1": "servicepoint.duckdns.org",
  "Domain2": "",
  "Port": 6755,
  "KeyboardLogging": "Enable",
  "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
HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x4d495:$name: ConfuserEx • 0x4cecb:$compile: AssemblyTitle

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x4d495:$name: ConfuserEx • 0x4cecb:$compile: AssemblyTitle

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x3e2ed:$x1: NanoCore.ClientPluginHost • 0x6666d:$x1: NanoCore.ClientPluginHost • 0x3e32a:$x2: IClientNetworkHost • 0x666aa:$x2: IClientNetworkHost • 0x41e5d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x6a1dd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x3e055:$a: NanoCore • 0x3e065:$a: NanoCore • 0x3e299:$a: NanoCore • 0x3e2ad:$a: NanoCore • 0x3e2ed:$a: NanoCore • 0x663d5:$a: NanoCore • 0x663e5:$a: NanoCore • 0x66619:$a: NanoCore • 0x6662d:$a: NanoCore • 0x6666d:$a: NanoCore • 0x3e0b4:$b: ClientPlugin • 0x3e2b6:$b: ClientPlugin • 0x3e2f6:$b: ClientPlugin • 0x66434:$b: ClientPlugin • 0x66636:$b: ClientPlugin • 0x66676:$b: ClientPlugin • 0x3e1db:$c: ProjectData • 0x6655b:$c: ProjectData • 0x3ebe2:$d: DESCrypto • 0x66f62:$d: DESCrypto • 0x465ae:$e: KeepAlive
00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x3e2ed:$a1: NanoCore.ClientPluginHost • 0x6666d:$a1: NanoCore.ClientPluginHost • 0x3e2ad:$a2: NanoCore.ClientPlugin • 0x6662d:$a2: NanoCore.ClientPlugin • 0x40206:$b1: get_BuilderSettings • 0x68586:$b1: get_BuilderSettings • 0x3e109:$b2: ClientLoaderForm.resources • 0x66489:$b2: ClientLoaderForm.resources • 0x3f926:$b3: PluginCommand • 0x67ca6:$b3: PluginCommand • 0x3e2de:$b4: IClientAppHost • 0x6665e:$b4: IClientAppHost • 0x4875e:$b5: GetBlockHash • 0x70ade:$b5: GetBlockHash • 0x4085e:$b6: AddHostEntry • 0x68bde:$b6: AddHostEntry • 0x44551:$b7: LogClientException • 0x6c8d1:$b7: LogClientException • 0x407cb:$b8: PipeExists • 0x68b4b:$b8: PipeExists • 0x3e317:$b9: IClientLoggingHost
00000001.00000002.516146416.00000000037A3000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x35756:$a: NanoCore • 0x3577b:$a: NanoCore • 0x357d4:$a: NanoCore • 0x4597f:$a: NanoCore • 0x459a5:$a: NanoCore • 0x45a01:$a: NanoCore • 0x5285f:$a: NanoCore • 0x528b8:$a: NanoCore • 0x528eb:$a: NanoCore • 0x52b17:$a: NanoCore • 0x52b93:$a: NanoCore • 0x531ac:$a: NanoCore • 0x532f5:$a: NanoCore • 0x537c9:$a: NanoCore • 0x53ab0:$a: NanoCore • 0x53ac7:$a: NanoCore • 0x5c96f:$a: NanoCore • 0x5c9eb:$a: NanoCore • 0x5f2ce:$a: NanoCore • 0x6489d:$a: NanoCore • 0x64917:$a: NanoCore
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.38574e0.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.38574e0.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.38574e0.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.38574e0.0.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe0f5:$x1: NanoCore Client • 0xe105:$x1: NanoCore Client • 0xe34d:$x2: NanoCore.ClientPlugin • 0xe38d:$x3: NanoCore.ClientPluginHost • 0xe342:$i1: IClientApp • 0xe363:$i2: IClientData • 0xe36f:$i3: IClientNetwork • 0xe37e:$i4: IClientAppHost • 0xe3a7:$i5: IClientDataHost • 0xe3b7:$i6: IClientLoggingHost • 0xe3ca:$i7: IClientNetworkHost • 0xe3dd:$i8: IClientUIHost • 0xe3eb:$i9: IClientNameObjectCollection • 0xe407:$i10: IClientReadOnlyNameObjectCollection • 0xe154:$s1: ClientPlugin • 0xe356:$s1: ClientPlugin • 0xe84a:$s2: EndPoint • 0xe853:$s3: IPAddress • 0xe85d:$s4: IPEndPoint • 0x10293:$s6: get_ClientSettings • 0x10837:$s7: get_Connected
0.2.HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.38574e0.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
Click to see the 77 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 Keepalive Response 1 - Source IP: 213.152.161.85 - Destination IP: 192.168.2.3 −

Timestamp:	213.152.161.85192.168.2.36755497052810290 02/04/23-04:02:37.885591
SID:	2810290

Source Port:	6755
Destination Port:	49705
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970067552816718 02/04/23-04:02:18.413039
SID:	2816718
Source Port:	49700
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971167552816766 02/04/23-04:03:22.114925
SID:	2816766
Source Port:	49711
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970867552816766 02/04/23-04:02:58.659576
SID:	2816766
Source Port:	49708
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971367552816766 02/04/23-04:03:34.873002
SID:	2816766
Source Port:	49713
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971367552816718 02/04/23-04:03:32.601666
SID:	2816718
Source Port:	49713
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971667552816766 02/04/23-04:03:58.093532
SID:	2816766
Source Port:	49716
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 213.152.161.85 - Destination IP: 192.168.2.3	
Timestamp:	213.152.161.85192.168.2.36755497122841753 02/04/23-04:03:27.123757
SID:	2841753
Source Port:	6755
Destination Port:	49712
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 213.152.161.85 - Destination IP: 192.168.2.3	
Timestamp:	213.152.161.85192.168.2.36755497032841753 02/04/23-04:02:24.159041
SID:	2841753
Source Port:	6755
Destination Port:	49703
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970567552816766 02/04/23-04:02:38.804523
SID:	2816766
Source Port:	49705
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971567552816766 02/04/23-04:03:50.787453
SID:	2816766
Source Port:	49715
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970767552816766 02/04/23-04:02:51.380389
SID:	2816766
Source Port:	49707
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970367552816766 02/04/23-04:02:24.379082
SID:	2816766
Source Port:	49703
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970967552816766 02/04/23-04:03:05.988800
SID:	2816766
Source Port:	49709
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971267552816766 02/04/23-04:03:27.448220
SID:	2816766
Source Port:	49712
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971767552816766 02/04/23-04:04:04.561310
SID:	2816766
Source Port:	49717

Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 213.152.161.85 - Destination IP: 192.168.2.3	
Timestamp:	213.152.161.85192.168.2.36755497112841753 02/04/23-04:03:22.044641
SID:	2841753
Source Port:	6755
Destination Port:	49711
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970067552816766 02/04/23-04:02:19.457207
SID:	2816766
Source Port:	49700
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970667552816766 02/04/23-04:02:45.198697
SID:	2816766
Source Port:	49706
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971467552816766 02/04/23-04:03:42.744453
SID:	2816766
Source Port:	49714
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854970467552816766 02/04/23-04:02:30.984485
SID:	2816766
Source Port:	49704
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 213.152.161.85	
Timestamp:	192.168.2.3213.152.161.854971067552816766 02/04/23-04:03:16.374407
SID:	2816766
Source Port:	49710
Destination Port:	6755
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

PE file has nameless sections

PE file contains section with special chars

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)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

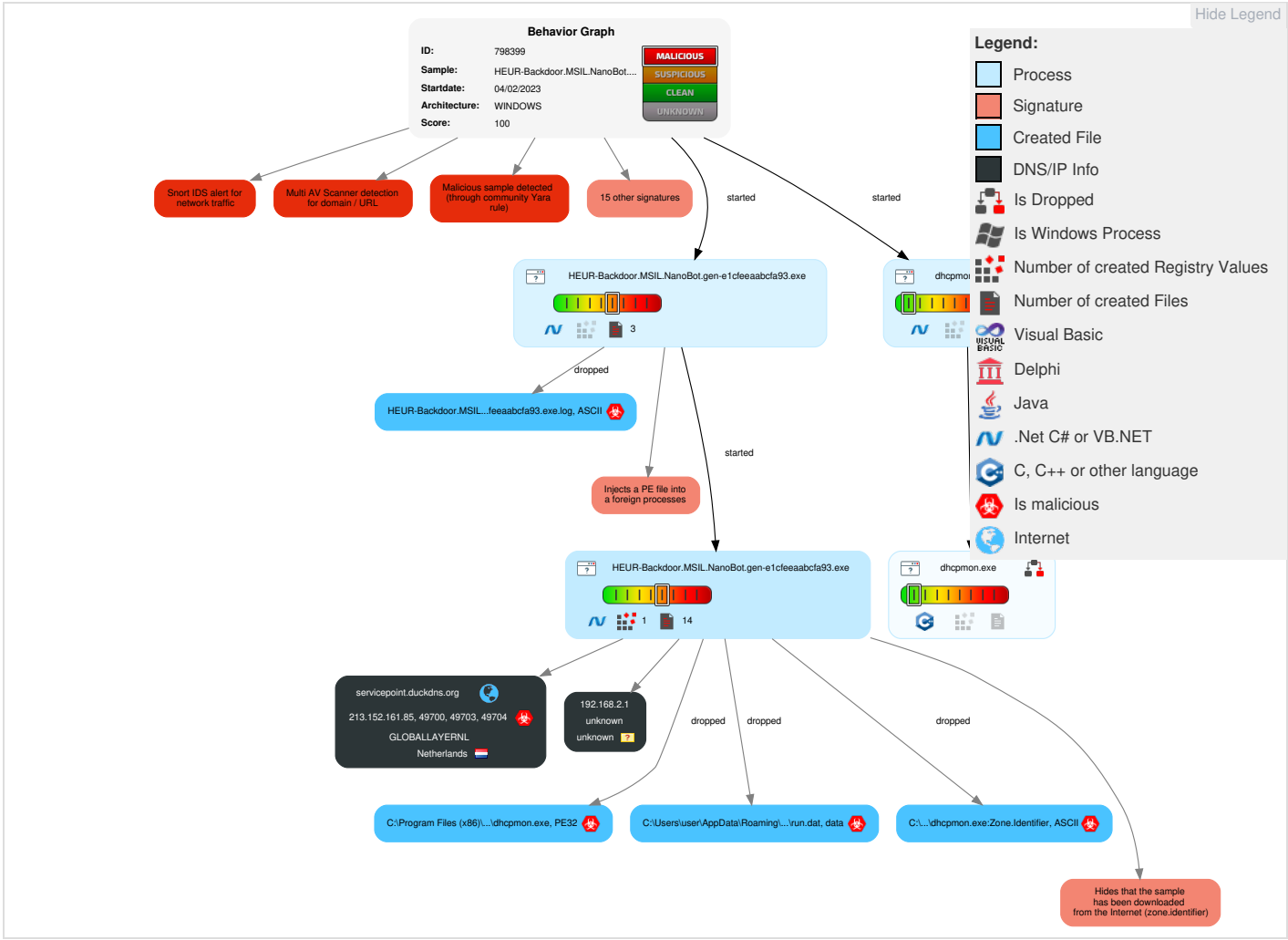
Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	2 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	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 1 2 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	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 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 2 Process Injection	LSA Secrets	2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	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 Hidden Files and Directories	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	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 2 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

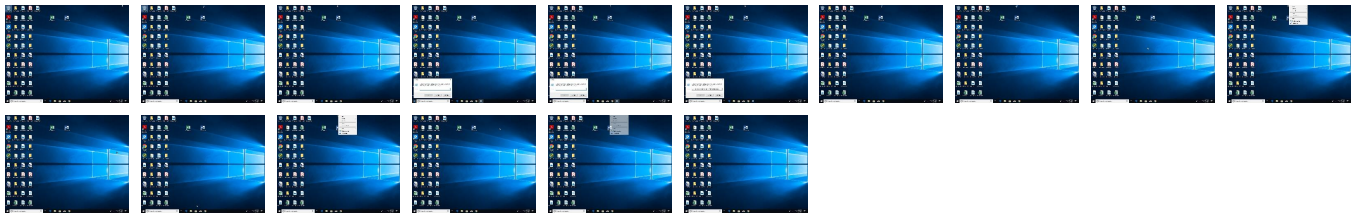
Behavior Graph



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
HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe	45%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe	57%	Virustotal		Browse
HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe	100%	Avira	HEUR/AGEN.1202424	
HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	HEUR/AGEN.1202424	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	45%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	57%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1208316		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.e0000.0.unpack	100%	Avira	HEUR/AGEN.1202424		Download File

Domains

Source	Detection	Scanner	Label	Link
servicepoint.duckdns.org	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
servicepoint.duckdns.org	100%	Avira URL Cloud	malware	
servicepoint.duckdns.org	11%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
servicepoint.duckdns.org	213.152.161.85	true	true	• 11%, Virustotal, Browse	unknown

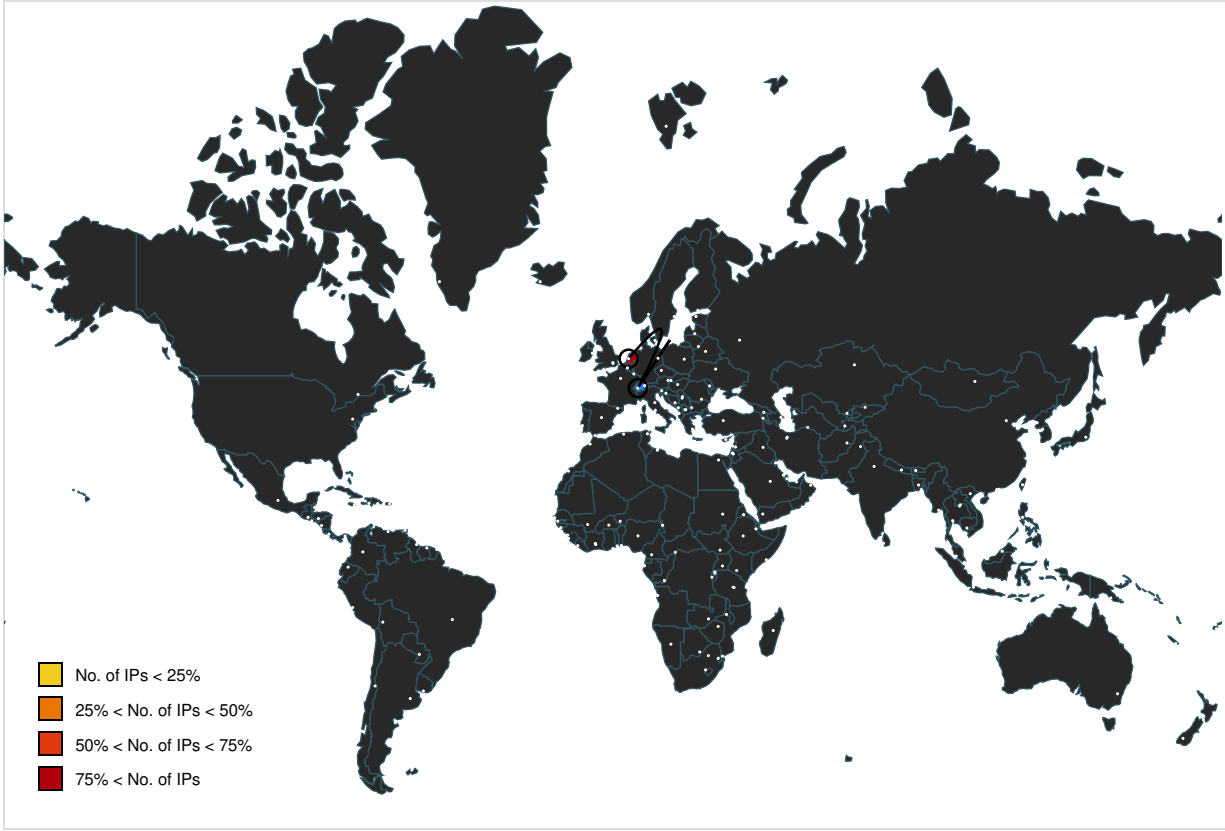
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
servicepoint.duckdns.org	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe, 00000001.00000002.516146416.00000000037A3000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.152.161.85	servicepoint.duckdns.org	Netherlands		49453	GLOBALLAYERNL	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	798399
Start date and time:	2023-02-04 04:01:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 15s
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:	15
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:	HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/8@16/2

EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Execution Graph export aborted for target HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe, PID 5368 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:02:01	API Interceptor	838x Sleep call for process: HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe modified
04:02:03	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
04:02:14	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	924672
Entropy (8bit):	6.4582092585373525
Encrypted:	false
SSDEEP:	12288:pLYT+m0qD8CEULAfPpIuG1JZnXiGDyQics5Ec0Y7JOfEhvlQd9DiTsOzLnWIKBlK:pE+K4ozvtYpjsBhX
MD5:	8C4F47A96A1F9F58AB28A2353627C153
SHA1:	4E7E9F7C7D630E2406FE76AD1576D35A773E9E06
SHA-256:	E1CFEEAABCFA9339523FAE340820F04895C7A8332B806FD4E813343516928DDE
SHA-512:	E251A5109139F7440F9E515F8132DC4116E59E29A0CDD2C9FC2DF2EE70B975EB6F8C1E373E5401C0B39A4D8BA9894EA3CCC7645E2C314214D787DFFF28D284 8
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Arnim Rupp
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 45% • Antivirus: Virustotal, Detection: 57%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.X.....P..... ....@.. .....'.. ..@.....`...K..... .....H.....4SU.P.}s..... .....@....text...H..... ..`.rsrc... ....I.....@..@.reloc.....@..B..... ..`..... ....

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

Process:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.log

Process:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5I 3
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.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.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.285418593366258
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2+gYhD5iv:MLF20NaL3z2p29hJ5g522rW2+g2+
MD5:	63CC04E8E9DBE6842611C2E6E948F8FA
SHA1:	61F604AF4DABFEC36C39555FE4A32D1D6417927C
SHA-256:	0EDC65EF06683A15D2C8B6A455F8A29B29AE729069096A060D6C75E12AB0EB60
SHA-512:	57A4B08AEC6F1663C50AFF9259EEBFA50CCE8C4B406555E8522DCCF1E0DA03DA3686AE8208045D4ADC574396B9D8AD87B6C0D64FACE82AC913D2EBEC9A1100E
Malicious:	false
Reputation:	moderate, 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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.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\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

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

Process:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7r3l3TmKEt5mT1DhFtMhXvvHOxHB3GDq:X4LEnybgCFCtvd7bl3ThE4T19FtMhXvs
MD5:	061E700FE27D852034A5A44BF5985CCF
SHA1:	15B072DE6D6FDD92AE36F074345FA41985833E8D
SHA-256:	4BBB88AF530693EB4A710B0591D4BAF585837242C5690F5A821BF2FC9CC587CD
SHA-512:	CF6C5458AB50C859740490985D1E7E887D1116F3FA947FF2EC49AF9997A42F3402C63EF42B93498544195D9859FBB19CCC295966564B30F5ADB4A36D4E8886C6
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.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.w

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

Process:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:nS:nS
MD5:	936600CAA6F0F7229FF1F3E8F92BE5EB
SHA1:	311583C4CA7235B76A80EBF66DABB67119877474
SHA-256:	2632A97CC041EF4110299290C537C046021994E5A5C0E5970D6C6A7E11F917CD
SHA-512:	247551FBCD4BD20952910B2B33BDA3674558D71A24C16B8F9162CCC8D032CB0E7CFA0C85EC63E12200D46ACDECD5484BBB3653B64CABDE1538F8B2BB2CB1AA0E
Malicious:	**true**
Preview:	......H

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

Process:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621

MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B3680189O7A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

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

Process:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File Type:	data
Category:	dropped
Size (bytes):	433688
Entropy (8bit):	**7.999519077450246**
Encrypted:	**true**
SSDEEP:	12288:dcRKtiKlC1FGhWjoORvi5oCILR9Eax5uoj:KRCiKECCGoD9Eaioj
MD5:	D2D87B1E9F691E38698A9683C9E213C1
SHA1:	87FAA25A212348CCD20567929D52A0ADE5BE07CE
SHA-256:	4115C31136A8A8F4642D3F5E7032A248381FCF36B047CFD911F974600F140039
SHA-512:	541F3C4C9CA97C085065FA5881D9A336F0BE474C90D1C65379CA7CB7F084B6496ED52A61F9133FD29DE5DB57C2B1F2CC302498579C5A158F823612EAC248C5DC
Malicious:	false
Preview:	.....O.....\8..5N..`S.]..[r.$*>.\.#v&..$.....Z.i..M.Mn5.@..@...3.R..Y...}>C.b....Z.....K..^.d...Z...K.#...dn$e ..XP.^.#.....V...dB.Kn.Y.c..-k....M.D...Q.S..R.X....._...Zz...#.=<.V.NHZq.h..ON..oq.:...,7H...../..Q..R.u6.."....<.`..z.5b($..9.CF.F1...o?.h.}....;Ay....kL}7...I.-}..D&...C....%.J..+..1.5.a..Ih....s.....G..?..9^0e...p..FCvNt.e...B/...y.h.G.0..o,Q.2[.....e.P8.....yr...*..Q..*..../..S..m.....\.wA.a1.]...oW.....PY..h....f:.....Ss.....\.8...@R._A...M..X....V.f).]z..u{.z-....W...NaT+.&:...1.D../.7..\.S..z..!.....#..F.d.....*.m'.....6.2....:H...bd]..._.....}.n.=...I.7%r.>...B.Q.K..q...Ex.6.6....P..^...i...Mx...;g...,t..fCd.\.b....e{.\...Y=4.....+..T....j}..|66g.s...z...Y.kTi..?Xy...5\...SO..W.U.3A.$.I..{.D...no.E..v.2.:..a..hdhO..t.w.k..T|Po.....D?..mG.[.2.;....+...8.6.h!..w.3...w.o.....\....f.v.to.B.{`o..a.....f.cu.....?.....".u..EA...^)W..z..jtU{^.....5#....y.s.....e.I..&...%...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.4582092585373525
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
File size:	924672
MD5:	8c4f47a96a1f9f58ab28a2353627c153
SHA1:	4e7e9f7c7d630e2406fe76ad1576d35a773e9e06
SHA256:	e1cfeeaabcfa9339523fae340820f04895c7a8332b806fd4e813343516928dde
SHA512:	e251a5109139f7440f9e515f8132dc4116e59e29a0cdd2c9fc2df2ee70b975eb6f8c1e373e5401c0b39a4d8ba9894ea3ccc7645e2c314214d787dfff28d28478
SSDEEP:	12288:pLYT+m0qD8CEULAfPpIuG1JZnXiGDyQics5Ec0Y7JOfEhvlQd9DiTsOzLnWIKBlK:pE+K4ozvtYpjsBhX
TLSH:	6C15FF9835203E9ECC5FC471DB791FE49E137E66430AC1D3643B29A9BA9C486CE543A3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.X.....P..... ....@.. .....'....@.....

File Icon

Icon Hash:	f0d6e66799bcc678

Static PE Info

General

Entrypoint:	0x4ea00a
Entrypoint Section:	
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x58016ADD [Fri Oct 14 23:31:41 2016 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 [004EA000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e860	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8c000	0x5ab20	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	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	0xea000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x1e000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
4SUP}s	0x2000	0x1a110	0x1a200	False	1.000383148923445	data	7.998441047887134	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.text	0x1e000	0x6c448	0x6c600	False	0.6105757100634371	data	6.673125048528245	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x5ab20	0x5ac00	False	0.11296918044077135	data	4.047706271353626	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xea000	0x10	0x200	False	0.046875	data	0.14263576814887827	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x8c1d8	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 262144		
RT_ICON	0xce200	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536		
RT_ICON	0xdea28	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384		
RT_ICON	0xe2c50	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0xe51f8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_ICON	0xe62a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024		
RT_GROUP_ICON	0xe6708	0x5a	data		
RT_VERSION	0xe6764	0x3bc	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

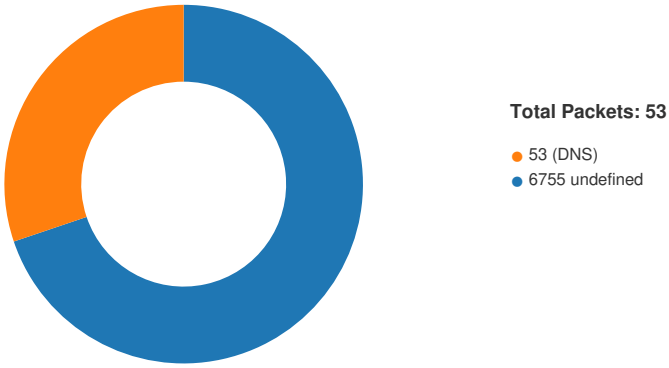
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
213.152.161.85192.168.2.36755497052810290 02/04/23-04:02:37.885591	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	6755	49705	213.152.161.85	192.168.2.3
192.168.2.3213.152.161.854970067552816718 02/04/23-04:02:18.413039	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49700	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854971167552816766 02/04/23-04:03:22.114925	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854970867552816766 02/04/23-04:02:58.659576	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854971367552816766 02/04/23-04:03:34.873002	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854971367552816718 02/04/23-04:03:32.601666	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49713	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854971667552816766 02/04/23-04:03:58.093532	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	6755	192.168.2.3	213.152.161.85
213.152.161.85192.168.2.36755497122841753 02/04/23-04:03:27.123757	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6755	49712	213.152.161.85	192.168.2.3
213.152.161.85192.168.2.36755497032841753 02/04/23-04:02:24.159041	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6755	49703	213.152.161.85	192.168.2.3
192.168.2.3213.152.161.854970567552816766 02/04/23-04:02:38.804523	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854971567552816766 02/04/23-04:03:50.787453	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854970767552816766 02/04/23-04:02:51.380389	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854970367552816766 02/04/23-04:02:24.379082	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854970967552816766 02/04/23-04:03:05.988800	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.854971267552816766 02/04/23-04:03:27.448220	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	6755	192.168.2.3	213.152.161.85

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3213.152.161.8549717675528167660 2/04/23-04:04:04.561310	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	6755	192.168.2.3	213.152.161.85
213.152.161.85192.168.2.36755497112841753 02/04/23-04:03:22.044641	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6755	49711	213.152.161.85	192.168.2.3
192.168.2.3213.152.161.8549700675528167660 2/04/23-04:02:19.457207	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49700	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.8549706675528167660 2/04/23-04:02:45.198697	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.8549714675528167660 2/04/23-04:03:42.744453	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.8549704675528167660 2/04/23-04:02:30.984485	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	6755	192.168.2.3	213.152.161.85
192.168.2.3213.152.161.8549710675528167660 2/04/23-04:03:16.374407	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	6755	192.168.2.3	213.152.161.85

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 04:02:04.611284971 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:07.613686085 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:13.629790068 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:15.676836967 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:15.680389881 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.111125946 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.205787897 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.205946922 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.322611094 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.322686911 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.392013073 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.420710087 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.528934002 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.529026031 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.638359070 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.658832073 CET	6755	49700	213.152.161.85	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 04:02:16.666656017 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.666857958 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.673273087 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.681354046 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.681562901 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.688656092 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.696311951 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.696590900 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.703542948 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.711205959 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.711426973 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.719104052 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.726268053 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.726416111 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.739782095 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.747046947 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.747176886 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.754599094 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.761791945 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.761902094 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.770402908 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.777575970 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.777683020 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.785461903 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.792680979 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.792895079 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.801043034 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.808748007 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.809031010 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.816339016 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.823241949 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.823446989 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.832508087 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.839982986 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.840135098 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.846998930 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.854598999 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.854706049 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.861953974 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.869898081 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.870024920 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.877110958 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.884836912 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.884959936 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.913599968 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.921849012 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.922086954 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.929075003 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.937515974 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.937809944 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.944855928 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.952564001 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.952915907 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.960236073 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.967772961 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.967920065 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:16.975361109 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.983282089 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.983412981 CET	49700	6755	192.168.2.3	213.152.161.85

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 04:02:16.991182089 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.998938084 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:16.999104023 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.006727934 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.014380932 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.014542103 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.022173882 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.029648066 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.029809952 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.037746906 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.045418978 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.045552015 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.053241968 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.060940981 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.061116934 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.069979906 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.077694893 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.077814102 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.085335016 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.093101978 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.093220949 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.100375891 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.108539104 CET	6755	49700	213.152.161.85	192.168.2.3
Feb 4, 2023 04:02:17.108741999 CET	49700	6755	192.168.2.3	213.152.161.85
Feb 4, 2023 04:02:17.116328955 CET	6755	49700	213.152.161.85	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 04:02:04.475367069 CET	49977	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:02:04.585163116 CET	53	49977	8.8.8.8	192.168.2.3
Feb 4, 2023 04:02:23.751883030 CET	57990	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:02:23.861915112 CET	53	57990	8.8.8.8	192.168.2.3
Feb 4, 2023 04:02:28.712673903 CET	52387	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:02:28.820549965 CET	53	52387	8.8.8.8	192.168.2.3
Feb 4, 2023 04:02:36.860551119 CET	56924	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:02:36.968187094 CET	53	56924	8.8.8.8	192.168.2.3
Feb 4, 2023 04:02:43.029052019 CET	60625	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:02:43.047238111 CET	53	60625	8.8.8.8	192.168.2.3
Feb 4, 2023 04:02:49.385057926 CET	49302	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:02:49.403115034 CET	53	49302	8.8.8.8	192.168.2.3
Feb 4, 2023 04:02:56.138262987 CET	53975	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:02:56.245413065 CET	53	53975	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:03.168420076 CET	51139	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:03.277697086 CET	53	51139	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:11.669126034 CET	52955	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:11.687891960 CET	53	52955	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:21.697429895 CET	60582	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:21.804183006 CET	53	60582	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:26.464158058 CET	57134	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:26.572953939 CET	53	57134	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:32.089087009 CET	62050	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:32.199491024 CET	53	62050	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:39.334427118 CET	56042	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:39.441394091 CET	53	56042	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:48.096045971 CET	59636	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:48.114181042 CET	53	59636	8.8.8.8	192.168.2.3
Feb 4, 2023 04:03:55.169281006 CET	55638	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:03:55.187141895 CET	53	55638	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 04:04:02.506531954 CET	57704	53	192.168.2.3	8.8.8.8
Feb 4, 2023 04:04:02.526576996 CET	53	57704	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 4, 2023 04:02:04.475367069 CET	192.168.2.3	8.8.8.8	0x38ce	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:23.751883030 CET	192.168.2.3	8.8.8.8	0xe29d	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:28.712673903 CET	192.168.2.3	8.8.8.8	0x6bc8	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:36.860551119 CET	192.168.2.3	8.8.8.8	0x1fc4	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:43.029052019 CET	192.168.2.3	8.8.8.8	0x9b90	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:49.385057926 CET	192.168.2.3	8.8.8.8	0xe464	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:56.138262987 CET	192.168.2.3	8.8.8.8	0x1c8c	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:03.168420076 CET	192.168.2.3	8.8.8.8	0xd889	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:11.669126034 CET	192.168.2.3	8.8.8.8	0x1f72	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:21.697429895 CET	192.168.2.3	8.8.8.8	0x3bb2	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:26.464158058 CET	192.168.2.3	8.8.8.8	0x4477	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:32.089087009 CET	192.168.2.3	8.8.8.8	0x6db4	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:39.334427118 CET	192.168.2.3	8.8.8.8	0xc4e7	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:48.096045971 CET	192.168.2.3	8.8.8.8	0x4382	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:55.169281006 CET	192.168.2.3	8.8.8.8	0x4de6	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:04:02.506531954 CET	192.168.2.3	8.8.8.8	0x627a	Standard query (0)	servicepoint.duckdns.org	A (IP address)	IN (0x0001)	false

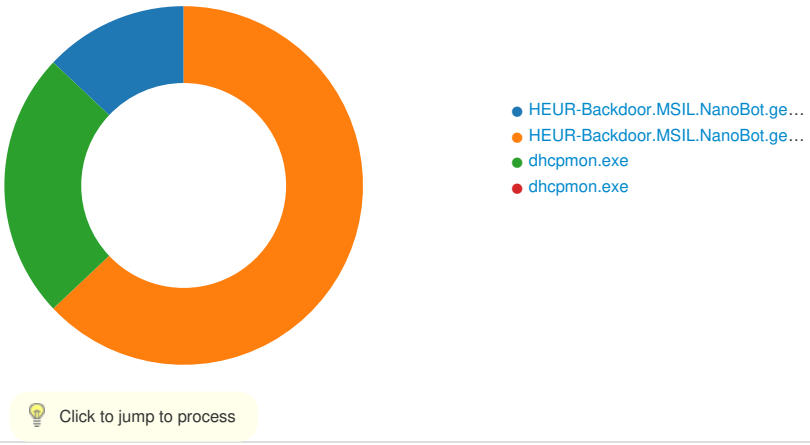
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 4, 2023 04:02:04.585163116 CET	8.8.8.8	192.168.2.3	0x38ce	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:23.861915112 CET	8.8.8.8	192.168.2.3	0xe29d	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:28.820549965 CET	8.8.8.8	192.168.2.3	0x6bc8	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:36.968187094 CET	8.8.8.8	192.168.2.3	0x1fc4	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:43.047238111 CET	8.8.8.8	192.168.2.3	0x9b90	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:49.403115034 CET	8.8.8.8	192.168.2.3	0xe464	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:02:56.245413065 CET	8.8.8.8	192.168.2.3	0x1c8c	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:03.277697086 CET	8.8.8.8	192.168.2.3	0xd889	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:11.687891960 CET	8.8.8.8	192.168.2.3	0x1f72	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 4, 2023 04:03:21.804183006 CET	8.8.8.8	192.168.2.3	0x3bb2	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:26.572953939 CET	8.8.8.8	192.168.2.3	0x4477	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:32.199491024 CET	8.8.8.8	192.168.2.3	0x6db4	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:39.441394091 CET	8.8.8.8	192.168.2.3	0xc4e7	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:48.114181042 CET	8.8.8.8	192.168.2.3	0x4382	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:03:55.187141895 CET	8.8.8.8	192.168.2.3	0x4de6	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false
Feb 4, 2023 04:04:02.526576996 CET	8.8.8.8	192.168.2.3	0x627a	No error (0)	servicepoint.duckdns.org		213.152.161.85	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe PID: **4864**, Parent PID: **3452**

General

Target ID:	0
Start time:	04:01:59
Start date:	04/02/2023
Path:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
Imagebase:	0xe0000
File size:	924672 bytes
MD5 hash:	8C4F47A96A1F9F58AB28A2353627C153
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: 00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.251706419.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.251706419.0000000003904000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.251706419.0000000003904000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.251706419.0000000003904000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.251706419.0000000003904000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.251706419.00000000038A7000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.251706419.00000000038A7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.251706419.00000000038A7000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.251706419.00000000038A7000.00000004.00000800.00020000.00000000.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	6C9760AC	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	6C9760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C9634A7	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\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	6CC4A33A	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	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C9A8738	ReadFile

Analysis Process: HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe PID: **5368**, Parent PID: **4864**

General

Target ID:	1
Start time:	04:02:01
Start date:	04/02/2023
Path:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe
Imagebase:	0xde0000
File size:	924672 bytes
MD5 hash:	8C4F47A96A1F9F58AB28A2353627C153
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000001.00000002.516146416.00000000037A3000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.516146416.00000000037A3000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.516146416.0000000003751000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.511625925.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.511625925.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.511625925.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.511625925.0000000000402000.00000040.00000400.00020000.00000000.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	6C9760AC	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	6C9760AC	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	5960D15	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	5960E0F	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	5960D15	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	5961094	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	5961094	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	5960D15	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	5960D15	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	6C9760AC	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	6C9760AC	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	11	5960E0F	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5960E0F	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5960E0F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe:Zone.Identifier	success or wait	1	5961265	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	fd 51 fd fd 06 fd 48	H	success or wait	1	5960FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 6a 01 58 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 06 00 00 50 07 00 00 00 00 00 0a fd 0e 00 00 fd 01 00 00 20 00 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 0e 00 00 04 00 00 fd 27 0e 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELjXP @ '@	success or wait	4	5961094	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	5961094	CopyFileW
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 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 5f 66 fd 5a 23 fd 7c fd 11 fd 40 48 6b 47 10 1f fd 31 47 fd fd 4f 2a 56 2e 15 0e eb fd 1f fd fd fd fd 70 7a fd fd fd fd 22 fd 0a 07 fd 72 fd fd 10 77 26 26 7c fd fd 63 fd fd 33 7d 7e fd fd fd 1d fd 7e fd f6 fd 6f 73 fd fd 66 fd 05 fd 12 fd fd fd 34 12 fd 31 fd 67 4a fd 27 fd 64 22 fd 4c fd 0b fd 41 fd 74 fd c7 fd 46 fd 7b fd 2b 14 fd 43 0c 7c 26 fd 77	Gjh\3A5x&i+c(1PPcLTAb4ht+Z\ i@3{grv+VB]PW4C}uLfZ#|@HkGGO*V.pz"rw&&|c3}~~osf41gJ'd"LAtF{C|&w	success or wait	14	5960FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	433688	fd fd fd 01 fd fd fd fd 10 4f 02 b7 4d 0e fd fd 19 5c 38 fd fd 35 4e fd fd 60 53 fd 5d fd fd 5b 72 fd 24 2a 3e fd 5c fd 23 76 26 fd fd 24 fd fd 19 fd fd fd fd 5a fd 69 fd fd 4d fd 4d 6e 35 1d 40 fd fd 40 fd 10 fd 33 fd 52 77 fd 59 6c fd fd 7d 3e 43 1e 62 fd fd 0a fd 5a fd fd fd fd fd 08 fd fd 4b fd fd 5e fd 64 fd fd fd 5a fd fd 13 4b fd 23 fd fd 1b 64 6e 24 65 20 0d fd 58 50 02 5e fd 23 fd 7d fd fd fd 17 fd 56 fd fd 12 64 42 fd 4b 6e fd 59 fd 63 0b fd 2d 6b fd 07 18 89 4d 0c 44 0a 0a fd 51 fd 53 fd fd 52 ad 58 fd fd 0e fd 17 05 fd 19 fd 1a 5f fd fd fd 5a 7a fd fd fd 23 08 3d 3c 08 56 fd 4e 48 5a 71 39 68 fd 13 4f 4e fd fd 6f 71 fd 3a fd 18 1f 2c 37 48 fd 07 fd fd fd fd 2f fd fd 51 fd 3f 52 1b 75 36 19 41 22 fd fd	O\85N`S] [r$*>\#v&$ZiMMn5@@3 RY}>CbZK^dZK#dn$e XP^#VdBKnYc-kMD QSRX_Zz#= <VNHZqhONoq:,7H/QRu 6"	success or wait	1	5960FC7	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 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 5f 66 fd 5a 23 fd 7c fd 11 fd 40 48 6b 47 10 1f fd 31 47 fd fd 4f 2a 56 2e 15 0e eb fd 1f fd fd fd fd 70 7a fd fd fd fd 22 fd 0a 07 fd 72 fd fd 10 77 26 26 7c fd fd 63 fd fd 33 7d 7e fd fd fd 1d fd 7e fd f6 fd 6f 73 fd fd 66 fd 05 fd 12 fd fd fd 34 12 fd 31 fd 67 4a fd 27 fd 64 22 fd 4c fd 0b fd 41 fd 74 fd c7 fd 46 fd 7b fd 2b 14 fd 43 0c 7c 26 fd 77	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLfZ#| @HkGGO*V.p z"rw&&|c3}~~osf41gJ'd"L AtF{C|&w	success or wait	2	5960FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	5960FC7	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	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C9A8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CA4BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CA4BF06	unknown
C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe	unknown	4096	success or wait	1	6CA4BF06	unknown
C:\Users\user\Desktop\HEUR-Backdoor.MSIL.NanoBot.gen-e1cfeeaabcfa93.exe	unknown	512	success or wait	1	6CA4BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5960FC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5960FC7	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	5961186	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **5240**, Parent PID: **3452**

General

Target ID:	2
Start time:	04:02:11
Start date:	04/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x610000
File size:	924672 bytes
MD5 hash:	8C4F47A96A1F9F58AB28A2353627C153
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Arnim Rupp
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 45%, ReversingLabs • Detection: 57%, Virustotal, Browse
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	6C9760AC	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	6C9760AC	unknown
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	6C9760AC	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	6C9760AC	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	6C9634A7	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	641	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e 6e	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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	6CC4A33A	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	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C9A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6C9A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	DCAEC7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	DCAEC7	ReadFile

Analysis Process: dhcpmon.exe PID: **5168**, Parent PID: **5240**

General

Target ID:	3
Start time:	04:02:15
Start date:	04/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	
File size:	924672 bytes
MD5 hash:	8C4F47A96A1F9F58AB28A2353627C153
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly