ID: 880637
Sample Name: file.exe
Cookbook: default.jbs
Time: 15:37:42
Date: 02/06/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 5
Threatname: NanoCore 5
Yara Signatures 5
Initial Sample 5
Memory Dumps 5
Unpacked PEs 6
Sigma Signatures 7
AV Detection 7
E-Banking Fraud 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
Public IPs 12
General Information 12
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\file.exe.log 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log 14
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 14
\Device\ConDrv 14
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Authenticode Signature 15
Entrypoint Preview 15
Data Directories 16

Sections 16
Resources 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 18
DNS Queries 18
DNS Answers 18
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: file.exePID: 5540, Parent PID: 3528 19
General 19
File Activities 19
File Created 19
File Written 19
File Read 20
Analysis Process: CasPol.exePID: 5688, Parent PID: 5540 20
General 20
Analysis Process: CasPol.exePID: 6688, Parent PID: 5540 20
General 20
Analysis Process: CasPol.exePID: 6672, Parent PID: 5540 21
General 21
Analysis Process: CasPol.exePID: 6636, Parent PID: 5540 21
General 21
File Activities 22
File Created 22
File Written 23
File Read 23
Registry Activities 24
Key Value Created 24
Analysis Process: dhcpmon.exePID: 7020, Parent PID: 3528 24
General 24
File Activities 24
File Created 24
File Written 24
File Read 25
Analysis Process: conhost.exePID: 5172, Parent PID: 7020 25
General 25
Disassembly 25

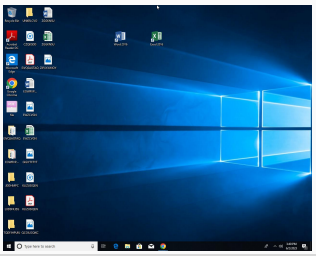
Windows Analysis Report

file.exe

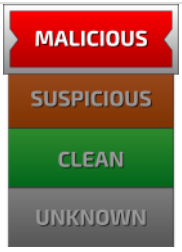
Overview

General Information

Sample Name:	file.exe
Analysis ID:	880637
MD5:	8d93c7903bfd5..
SHA1:	fad787dd1ebae..
SHA256:	685522dda736...
Tags:	NET exe MSIL x64 zgRAT
Infos:	



Detection



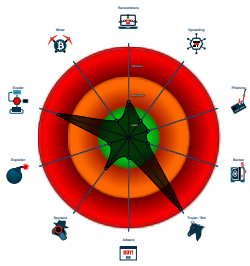
Nanocore, zgRAT

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- 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…
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- .NET source code references suspic…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5540 cmdline: C:\Users\user\Desktop\file.exe MD5: 8D93C7903BFD5900D72DBEB3B0968508)
  - CasPol.exe (PID: 5688 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 6688 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 6672 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 6636 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
- dhcpmon.exe (PID: 7020 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: F866FC1C2E928779C7119353C3091F0C)
  - conhost.exe (PID: 5172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **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

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
zgRAT		No Attribution	http://https://bazaar.abuse.ch/browse/signature/zgRAT/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.zgrat

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "954449b5-566c-46fe-92f0-8eb82a7f",
  "Group": "Cashout",
  "Domain1": "ezemnia3.ddns.net",
  "Domain2": "91.193.75.178",
  "Port": 62335,
  "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
file.exe	JoeSecurity_zgRAT_1	Yara detected zgRAT	Joe Security	
file.exe	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x1011f:$s1: file:/// • 0x1002d:$s2: {11111-22222-10009-11112} • 0x100af:$s3: {11111-22222-50001-00000} • 0xf54d:$s4: get_Module • 0xbf35:$s5: Reverse • 0xe4d6:$s6: BlockCopy • 0xc27b:$s7: ReadByte • 0x10131:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.808605429.0000000003F29000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.808605429.0000000003F29000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2f0d:$a: NanoCore • 0x2f66:$a: NanoCore • 0x2fa3:$a: NanoCore • 0x301c:$a: NanoCore • 0x166c7:$a: NanoCore • 0x166dc:$a: NanoCore • 0x16711:$a: NanoCore • 0x2f18b:$a: NanoCore • 0x2f1a0:$a: NanoCore • 0x2f1d5:$a: NanoCore • 0x2f6f:$b: ClientPlugin • 0x2fac:$b: ClientPlugin • 0x38aa:$b: ClientPlugin • 0x38b7:$b: ClientPlugin • 0x16483:$b: ClientPlugin • 0x1649e:$b: ClientPlugin • 0x164ce:$b: ClientPlugin • 0x166e5:$b: ClientPlugin • 0x1671a:$b: ClientPlugin • 0x2ef47:$b: ClientPlugin • 0x2ef62:$b: ClientPlugin
00000006.00000002.808605429.0000000003F29000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2fa3:$a1: NanoCore.ClientPluginHost • 0x16711:$a1: NanoCore.ClientPluginHost • 0x2f1d5:$a1: NanoCore.ClientPluginHost • 0x2f66:$a2: NanoCore.ClientPlugin • 0x166dc:$a2: NanoCore.ClientPlugin • 0x2f1a0:$a2: NanoCore.ClientPlugin • 0x333a:$b1: get_BuilderSettings • 0x1b657:$b1: get_BuilderSettings • 0x3411b:$b1: get_BuilderSettings • 0x2ff1:$b4: IClientAppHost • 0x33ab:$b6: AddHostEntry • 0x341a:$b7: LogClientException • 0x1b5c6:$b7: LogClientException • 0x3408a:$b7: LogClientException • 0x338f:$b8: PipeExists • 0x2fde:$b9: IClientLoggingHost • 0x1672b:$b9: IClientLoggingHost • 0x2f1ef:$b9: IClientLoggingHost
00000006.00000002.809329944.00000000051F0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000006.00000002.809329944.00000000051F0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.CasPol.exe.5d90000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
6.2.CasPol.exe.5d90000.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
6.2.CasPol.exe.5d90000.7.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
6.2.CasPol.exe.5d90000.7.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin • 0x147a2:$s6: get_ClientSettings
6.2.CasPol.exe.5d90000.7.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xf7ad:$a1: NanoCore.ClientPluginHost • 0xf778:$a2: NanoCore.ClientPlugin • 0x146f3:$b1: get_BuilderSettings • 0x14662:$b7: LogClientException • 0xf7c7:$b9: IClientLoggingHost
Click to see the 61 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

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking

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)

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

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

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected zgRAT

Yara detected Nanocore RAT

Remote Access Functionality

Yara detected zgRAT

Detected Nanocore Rat

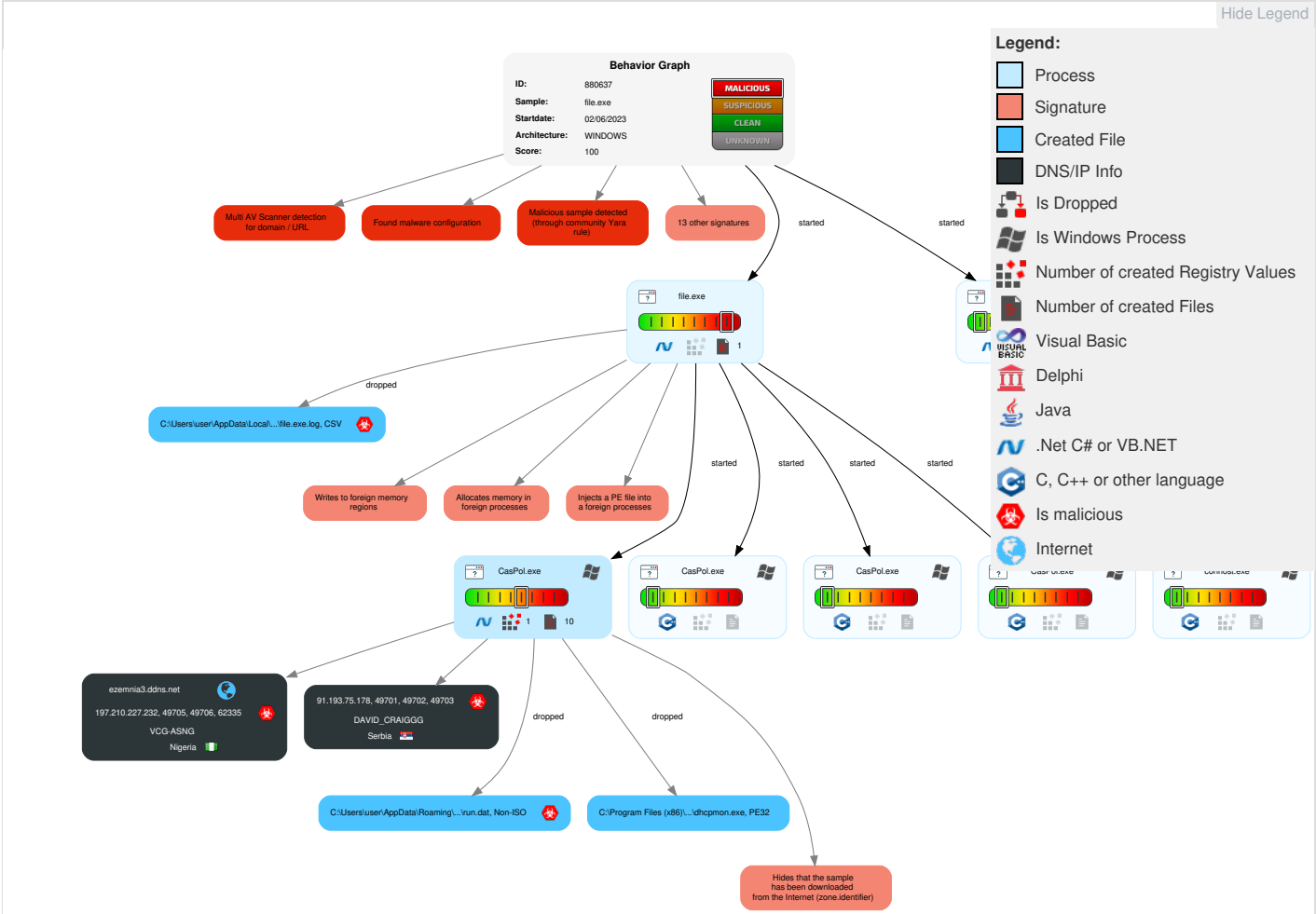
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	3 1 2 Process Injection	2 Masquerading	1 1 Input Capture	1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/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

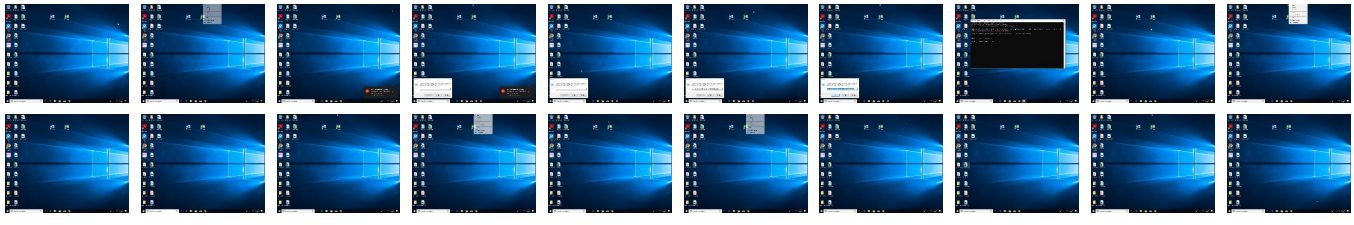
Behavior Graph

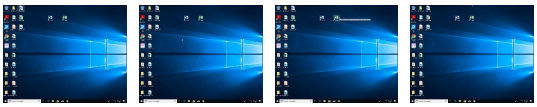


Screenshots

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
file.exe	43%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
file.exe	39%	Virustotal		Browse
file.exe	100%	Avira	HEUR/AGEN.1325558	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ezemnia3.ddns.net	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
ezemnia3.ddns.net	7%	Virustotal		Browse
91.193.75.178	13%	Virustotal		Browse
ezemnia3.ddns.net	100%	Avira URL Cloud	malware	
91.193.75.178	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ezemnia3.ddns.net	197.210.227.232	true	true	• 7%, Virustotal, Browse	unknown

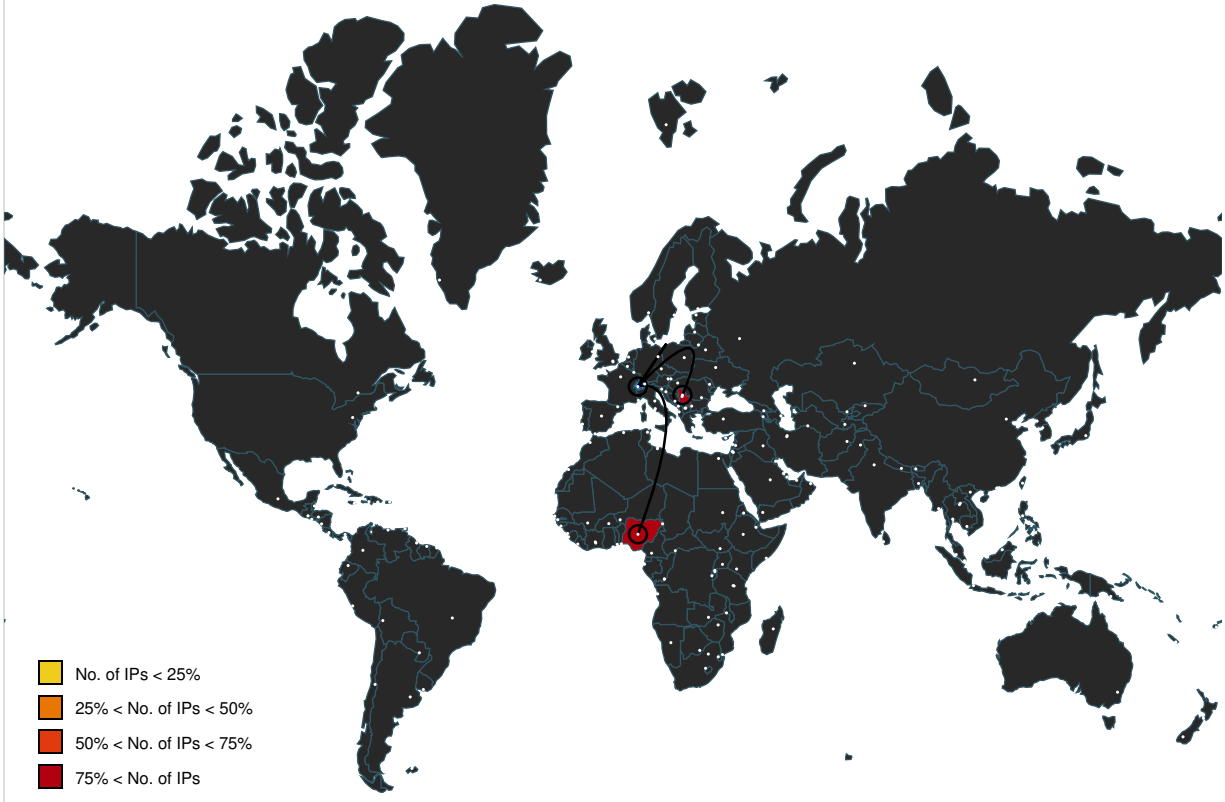
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ezemnia3.ddns.net	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	unknown
91.193.75.178	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 00000006.00000002.805344954.0000000002F37000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.210.227.232	ezemnia3.ddns.net	Nigeria		29465	VCG-ASNG	true
91.193.75.178	unknown	Serbia		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	880637
Start date and time:	2023-06-02 15:37:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 48s
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:	9
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:	file.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/5@6/2
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 23.3% (good quality ratio 19.9%) • Quality average: 56.3% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 80% • 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): audiodg.exe, WMIADAP.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Execution Graph export aborted for target dhcpmon.exe, PID 7020 because it is empty
- Execution Graph export aborted for target file.exe, PID 5540 because it is empty
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
15:38:43	API Interceptor	1003x Sleep call for process: CasPol.exe modified
15:38:44	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	107624
Entropy (8bit):	5.882571203162287
Encrypted:	false
SSDEEP:	1536:oSF7vA1hRqHixxMjlI34j8p2mdc/6A4vW/CU1RPMRVQJE:/A1hDPMip2mdcyA4vW/JRPMLQW
MD5:	F866FC1C2E928779C7119353C3091F0C
SHA1:	70D06064E2F12CFB10A82BC985F86F58EA7A4138
SHA-256:	67F3FC243C58EEAE55BDDC22CE025B7841A89ACA2E201B999D8C0E4F07D177B8
SHA-512:	B28B10801580726B85AB5F796EA26835648A3ACFBE1FBA95DFC687439B43FF9548BD3AB9EFC85D88FC071D232718BCFFAC614CC5BFF159173996A3D2AB22154D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...rX.Z.....0..X.....v... .....@.. ....Q.....`.....<v..O.....$.....f..h>.....u..... ..... ..H.....text....V... ...X..... ..`.rsrc...$.....Z..... ..@..@.reloc.....d.....@..B.....pv.....H.....,...`.....xE...t.....2~P....o....*.r...p(....*VrK..p(....s.....P...*..0..._.....~.....:O....>.....% .rm..p...A...s.....su....%.r...p...A...s....rm..p.su....%.r...p...B...s.....su....%.r...p...B...s....r...p.su....%.r...p...C...s.....su....%.r...p...C...s....r...p.su....%.r...p...D...s.....su....%.r...p... D...s....r...p.su....%.r...p...E...s.....su....%..r...p...E...s....r...p.su....%..r...p...F...s.....su....%..r...p...F

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

Process:	C:\Users\user\Desktop\file.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZiIv:Q3La/KDLI4MWuPTxAlv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	**true**

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177CE
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:YD:YD
MD5:	B9FAA684C030A959ECE6EDA0744AFD35
SHA1:	1CF54F509326FE102FC5EAEDB7A40FD01596867B
SHA-256:	473C5B472D03FC596D7FD7A483C62F9A54E839F21F81C8C21F5222A800F1C8E3
SHA-512:	6F50C9464093DA3735B6DF7E4F076A1C92CDFC14BC1B03D287EAC4F622130E9FE65EB4B168A3F30B8BA69C7FC42111566766BD84DC137E6EA2AFC82AB694BFA0
Malicious:	**true**
Preview:	....nc.H

\Device\ConDrv

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	486
Entropy (8bit):	5.064987733454706
Encrypted:	false
SSDEEP:	12:z30U30b4BFNY8fNFquci7S1pE+DPOCN6+QOH5JyY:z3F3g4DO4UE+Tz5JB
MD5:	30394F72BB157162F35A2DEB1F48BD1A
SHA1:	66AD7D748F42C64E0698606A8F019D165DE657E8
SHA-256:	133FABF0CD558FA3E5144E9EF35654FA0422F8424C6D5D82828B8D10EC9BA295
SHA-512:	A93E12D6C9927403FE0E20B8A698B24007EBCCD53A29AD65428366C6CE3CED05E5F3AEFF1D46C7D9F174EAEAE5059F0B5D12353B6022965CDC5D187E45FA72E9
Malicious:	false
Preview:	Microsoft .NET Framework CasPol 4.7.3056.0..for Microsoft .NET Framework version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....WARNING: The .NET Framework does not apply CAS policy by default. Any settings shown or modified by CasPol will only ..affect applications that opt into using CAS policy. .... Please see http://go.microsoft.com/fwlink/?LinkId=131738 for more information. ......ERROR: Not enough arguments....For usage information, use 'caspol -?'..

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.944928855592647

TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	file.exe
File size:	834112
MD5:	8d93c7903bfd5900d72dbeb3b0968508
SHA1:	fad787dd1ebae5cc64aaf7762dd6f49de50adfa7
SHA256:	685522dda736e8c071fcc9dc4b7bb3d58c45f36828eb0b8ca8557e5ec56499ad
SHA512:	c6a36b15350a8579d81f6d9fa9b3f069251dcee996f2047a2b6c60bd4c1705b4bb1a3a954ead68378119c460db385a554901950a7240ca40b54ed589d9bf46e1
SSDEEP:	24576:0mr0x3EEEfgYsSKS+KY9Zl6IX+OPZjv8+i0YUlo4:0mry3EEWKHrLPZjvpzlo4
TLSH:	070512697744348DC81BC8B1D9EA0C3167A277AB6777C3073147128E8E87D6CF581A6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....X.....0..T..... ....@..... .....i....`...@.....@..... .....

File Icon

Icon Hash:	526c6a52d0e4f047

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xC358B1DE [Wed Nov 8 12:30:22 2073 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:	

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 12/13/2021 1:00:00 AM 1/9/2025 12:59:59 AM
Subject Chain	• CN=philandro Software GmbH, O=philandro Software GmbH, L=Stuttgart, S=Baden-W\xfcrttemberg, C=DE
Version:	3
Thumbprint MD5:	EAE713DFC05244CF4301BF1C9F68B1BE
Thumbprint SHA-1:	9CD1DDB78ED05282353B20CDFE8FA0A4FB6C1ECE
Thumbprint SHA-256:	9D7620A4CEBA92370E8828B3CB1007AEFF63AB36A2CBE5F044FDDE14ABAB1EBF
Serial:	0DBF152DEAF0B981A8A938D53F769DB8

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al

Instruction
add byte ptr [eax], al
add byte ptr [eax+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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x1c1a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xc7400	0x4640	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc7388	0x1c	.text
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc53d0	0xc5400	False	0.9533168468789607	data	7.952638566367337	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x1c1a	0x1e00	False	0.33098958333333334	data	5.310141871037977	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

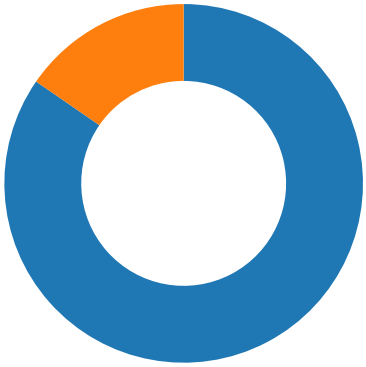
Name	RVA	Size	Type	Language	Country
RT_ICON	0xc81b0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0xc9258	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0xc96c0	0x22	data		
RT_VERSION	0xc96e4	0x34c	data		
RT_MANIFEST	0xc9a30	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Network Behavior

Network Port Distribution

Total Packets: 39

- 53 (DNS)
- 62335 undefined



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 15:38:45.180541039 CEST	49695	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:38:48.188280106 CEST	49695	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:38:54.189002037 CEST	49695	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:39:05.644177914 CEST	49696	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:39:08.658771038 CEST	49696	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:39:14.659281969 CEST	49696	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:39:24.280808926 CEST	49700	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:39:27.285420895 CEST	49700	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:39:33.285824060 CEST	49700	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:39:42.834573030 CEST	49701	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:42.879101038 CEST	62335	49701	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:43.380434990 CEST	49701	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:43.425004959 CEST	62335	49701	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:43.927361965 CEST	49701	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:43.972152948 CEST	62335	49701	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:47.977063894 CEST	49702	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:48.021768093 CEST	62335	49702	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:48.537118912 CEST	49702	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:48.581811905 CEST	62335	49702	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:49.099692106 CEST	49702	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:49.144428968 CEST	62335	49702	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:53.149203062 CEST	49703	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:53.193831921 CEST	62335	49703	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:53.709573030 CEST	49703	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:53.754199982 CEST	62335	49703	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:54.257426023 CEST	49703	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:39:54.301930904 CEST	62335	49703	91.193.75.178	192.168.2.4
Jun 2, 2023 15:39:58.480582952 CEST	49704	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:01.491422892 CEST	49704	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:07.507503986 CEST	49704	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:17.230046034 CEST	49705	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:20.243091106 CEST	49705	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:26.243532896 CEST	49705	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:26.515712976 CEST	62335	49705	197.210.227.232	192.168.2.4
Jun 2, 2023 15:40:30.753041983 CEST	49706	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:30.930021048 CEST	62335	49706	197.210.227.232	192.168.2.4
Jun 2, 2023 15:40:31.431394100 CEST	49706	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:31.612078905 CEST	62335	49706	197.210.227.232	192.168.2.4
Jun 2, 2023 15:40:32.119024038 CEST	49706	62335	192.168.2.4	197.210.227.232
Jun 2, 2023 15:40:32.291821003 CEST	62335	49706	197.210.227.232	192.168.2.4
Jun 2, 2023 15:40:36.308774948 CEST	49707	62335	192.168.2.4	91.193.75.178

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 15:40:36.353142023 CEST	62335	49707	91.193.75.178	192.168.2.4
Jun 2, 2023 15:40:36.869467020 CEST	49707	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:40:36.913860083 CEST	62335	49707	91.193.75.178	192.168.2.4
Jun 2, 2023 15:40:37.416409016 CEST	49707	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:40:37.460726976 CEST	62335	49707	91.193.75.178	192.168.2.4
Jun 2, 2023 15:40:41.466217041 CEST	49708	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:40:41.513715029 CEST	62335	49708	91.193.75.178	192.168.2.4
Jun 2, 2023 15:40:42.026073933 CEST	49708	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:40:42.070286989 CEST	62335	49708	91.193.75.178	192.168.2.4
Jun 2, 2023 15:40:42.572973013 CEST	49708	62335	192.168.2.4	91.193.75.178
Jun 2, 2023 15:40:42.617302895 CEST	62335	49708	91.193.75.178	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 15:38:45.139378071 CEST	52239	53	192.168.2.4	8.8.8.8
Jun 2, 2023 15:38:45.165621996 CEST	53	52239	8.8.8.8	192.168.2.4
Jun 2, 2023 15:39:05.603955030 CEST	56807	53	192.168.2.4	8.8.8.8
Jun 2, 2023 15:39:05.639246941 CEST	53	56807	8.8.8.8	192.168.2.4
Jun 2, 2023 15:39:24.258562088 CEST	59444	53	192.168.2.4	8.8.8.8
Jun 2, 2023 15:39:24.279351950 CEST	53	59444	8.8.8.8	192.168.2.4
Jun 2, 2023 15:39:58.447350979 CEST	55570	53	192.168.2.4	8.8.8.8
Jun 2, 2023 15:39:58.473865986 CEST	53	55570	8.8.8.8	192.168.2.4
Jun 2, 2023 15:40:17.157872915 CEST	64906	53	192.168.2.4	8.8.8.8
Jun 2, 2023 15:40:17.197916031 CEST	53	64906	8.8.8.8	192.168.2.4
Jun 2, 2023 15:40:30.706660032 CEST	59446	53	192.168.2.4	8.8.8.8
Jun 2, 2023 15:40:30.741974115 CEST	53	59446	8.8.8.8	192.168.2.4

DNS Queries

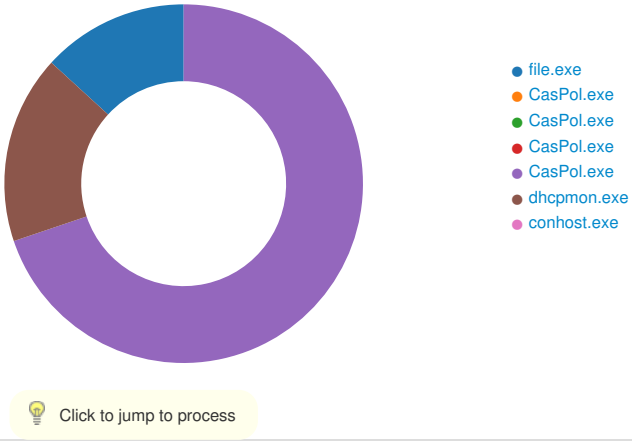
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 2, 2023 15:38:45.139378071 CEST	192.168.2.4	8.8.8.8	0xfd5	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:39:05.603955030 CEST	192.168.2.4	8.8.8.8	0xb8b7	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:39:24.258562088 CEST	192.168.2.4	8.8.8.8	0x154c	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:39:58.447350979 CEST	192.168.2.4	8.8.8.8	0xfe37	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:40:17.157872915 CEST	192.168.2.4	8.8.8.8	0x9593	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:40:30.706660032 CEST	192.168.2.4	8.8.8.8	0xbb35	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 15:38:45.165621996 CEST	8.8.8.8	192.168.2.4	0xfd5	No error (0)	ezemnia3.ddns.net		197.210.227.232	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:39:05.639246941 CEST	8.8.8.8	192.168.2.4	0xb8b7	No error (0)	ezemnia3.ddns.net		197.210.227.232	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:39:24.279351950 CEST	8.8.8.8	192.168.2.4	0x154c	No error (0)	ezemnia3.ddns.net		197.210.227.232	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:39:58.473865986 CEST	8.8.8.8	192.168.2.4	0xfe37	No error (0)	ezemnia3.ddns.net		197.210.227.232	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:40:17.197916031 CEST	8.8.8.8	192.168.2.4	0x9593	No error (0)	ezemnia3.ddns.net		197.210.227.232	A (IP address)	IN (0x0001)	false
Jun 2, 2023 15:40:30.741974115 CEST	8.8.8.8	192.168.2.4	0xbb35	No error (0)	ezemnia3.ddns.net		197.210.227.232	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **5540**, Parent PID: **3528**

General

Target ID:	0
Start time:	15:38:37
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x145c1610000
File size:	834112 bytes
MD5 hash:	8D93C7903BFD5900D72DBEB3B0968508
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: 00000000.00000002.549824099.00000145D4A79000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.549824099.00000145D4A79000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.549824099.00000145D4A79000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.549824099.00000145D4A79000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF875D986ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\file.exe.log	0	226	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0	success or wait	1	7FF875D98769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8757FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8757FB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8758D12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF875802625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8758D12E7	ReadFile

Analysis Process: CasPol.exe PID: **5688**, Parent PID: **5540**

General

Target ID:	3
Start time:	15:38:39
Start date:	02/06/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe
Imagebase:	0x330000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **6688**, Parent PID: **5540**

General

Target ID:	4
Start time:	15:38:40
Start date:	02/06/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe
Imagebase:	0x150000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **6672**, Parent PID: **5540**

General

Target ID:	5
Start time:	15:38:40
Start date:	02/06/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe
Imagebase:	0x100000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **6636**, Parent PID: **5540**

General

Target ID:	6
Start time:	15:38:40
Start date:	02/06/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe
Imagebase:	0x800000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.808605429.0000000003F29000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.808605429.0000000003F29000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.808605429.0000000003F29000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.809329944.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.809329944.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.809329944.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.809329944.00000000051F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.803937571.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.803937571.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.803937571.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.803937571.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.805344954.0000000002F37000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.809497378.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.809497378.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.809497378.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.809497378.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.809497378.0000000005D90000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71D6BEFF	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	71D61E60	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	71D6BEFF	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	71D6DD66	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	71D6BEFF	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	71D6BEFF	CreateDirectoryW

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 fd fd fd 6e 63 fd 48	ncH	success or wait	1	71D61B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	107624	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 72 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 58 01 00 00 0c 00 00 00 00 00 00 fd 76 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 51 fd 02 00 03 00 60 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.$PELrXZ0Xv @ Q`	success or wait	1	71D6DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72DFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	71D61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	71D61B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	512	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72DF5705	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	71D6646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **7020**, Parent PID: **3528**

General

Target ID:	7
Start time:	15:38:52
Start date:	02/06/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xa20000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71D61B4F	WriteFile
\Device\ConDrv	44	44	66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35	for Microsoft .NET Framework version 4.7.305	success or wait	10	71D61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	444	29	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75 73 65 20	For usage information, use	success or wait	2	71D61B4F	WriteFile
\Device\ConDrv	486	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71D61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	42	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",1	success or wait	1	7312C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile

Analysis Process: conhost.exe PID: **5172**, Parent PID: **7020**

General

Target ID:	8
Start time:	15:38:52
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly