ID: 881404
Sample Name: NA.exe
Cookbook: default.jbs
Time: 17:40:28
Date: 04/06/2023
Version: 37.1.0 Beryl

Table of Contents

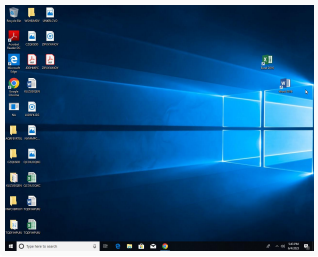
Windows Analysis Report

NA.exe

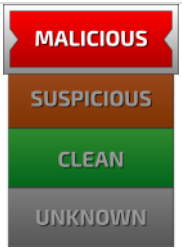
Overview

General Information

Sample Name:	NA.exe
Analysis ID:	881404
MD5:	6c432a8b26bc…
SHA1:	318fdcf5ba0a3…
SHA256:	0b525aaa05e2…
Tags:	exe
Infos:	



Detection



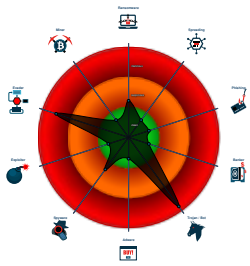
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- .NET source code references suspic…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- NA.exe (PID: 1544 cmdline: C:\Users\user\Desktop\NA.exe MD5: 6C432A8B26BC0E068F23E88F69C0F565)
  - CasPol.exe (PID: 5528 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
- dhcpmon.exe (PID: 4584 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: F866FC1C2E928779C7119353C3091F0C)
  - conhost.exe (PID: 7148 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

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.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
00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
00000001.00000002.650425425.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.CasPol.exe.5ce0000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
1.2.CasPol.exe.5ce0000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
1.2.CasPol.exe.5ce0000.5.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
1.2.CasPol.exe.5ce0000.5.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
1.2.CasPol.exe.5d70000.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 57 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 detection for URL or domain

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 Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

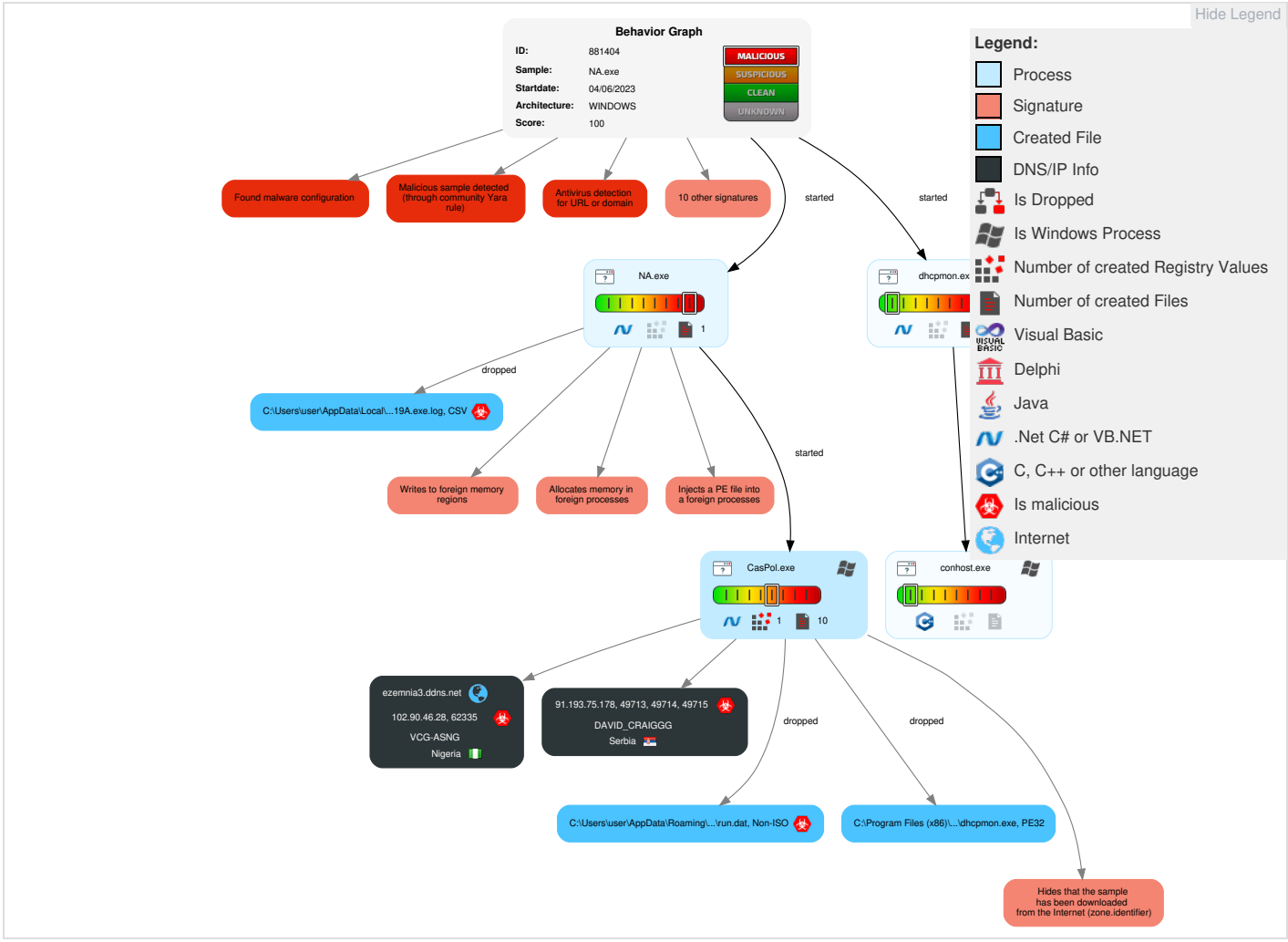
Yara detected Nanocore RAT

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 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
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

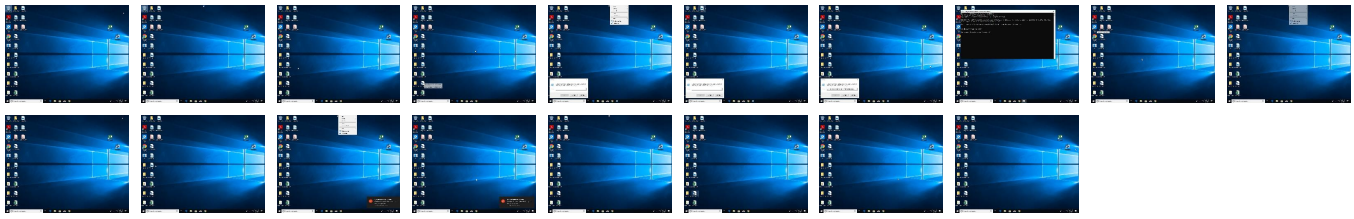
Behavior Graph



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
NA.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Heraclès	
NA.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

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ezemnia3.ddns.net	102.90.46.28	true	true		unknown

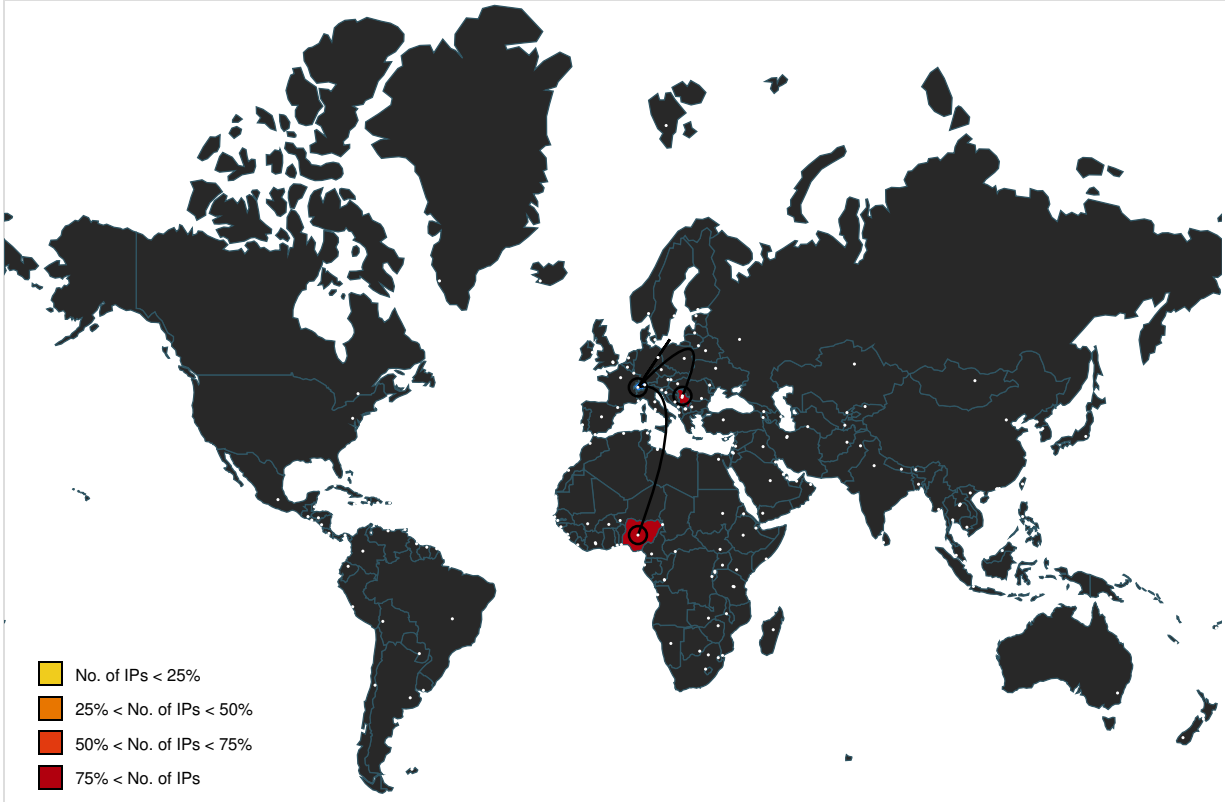
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ezemnia3.ddns.net	true	• Avira URL Cloud: malware	unknown
91.193.75.178	true	• 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, 00000001.00000002.651668667.0000000002E91000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	881404
Start date and time:	2023-06-04 17:40:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
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:	7
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:	NA.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@5/5@6/2
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 55.1% (good quality ratio 49.8%) • Quality average: 64.2% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 23.0.174.114, 23.0.174.96, 23.0.174.106, 23.0.174.107, 23.0.174.112, 23.0.174.97, 23.0.174.104, 23.0.174.91, 23.0.174.98
- Excluded domains from analysis (whitelisted): www.bing.com, e86303.dscx.akamaiedge.net, www.bing.com.edgekey.net, ctldl.windowsupdate.com, www-www.bing.com.trafficmanager.net
- Execution Graph export aborted for target NA.exe, PID 1544 because it is empty
- Execution Graph export aborted for target dhcpmon.exe, PID 4584 because it is empty
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: NA.exe

Simulations

Behavior and APIs

Time	Type	Description
17:41:28	API Interceptor	1054x Sleep call for process: CasPol.exe modified
17:41:30	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%
Reputation:	moderate, very likely benign file
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\NA.exe.log

Process:	C:\Users\user\Desktop\NA.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**
Reputation:	high, very likely benign file
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
Reputation:	high, very likely benign file
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, with escape sequences
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:yt:yt
MD5:	E4A6D16D7F7D253314AEF24A15FBC92A
SHA1:	8D34EBADE8A34A2C7393ED889B645FFFEC163048
SHA-256:	8ECF592FB6C70B0DF6F5C97FDDF4560224D9FF38F30443B50EFED9A99DBA0A31
SHA-512:	E4497B0F82D2E8D07308047409DA25CF15B838DB974E1E19BB15D29DCDC12631F16A9F2F0B35959F87874BF50433FAFC8C1434969736EFF833D27F5D82CB6332
Malicious:	**true**
Preview:	....]e.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):	7.963481307928194
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:	NA.exe
File size:	775680
MD5:	6c432a8b26bc0e068f23e88f69c0f565
SHA1:	318fdcf5ba0a326bf6601e1f917f9aa16645d9ca

SHA256:	0b525aaa05e206258e8e98f05fcc621a0c8d4df69138970a1447e57d157c6331
SHA512:	1a57c2c54e51a4e9bc1abf375a10e87236c5136cbbca0920597ecbf7f0d3bae674cced351ee5794028f7e7e25982bcb3409fc36d6ccf41b9497bbdec03a19c7e
SSDEEP:	12288:faNp9CFWv60PaT5zePZMjFkA1pniuSwgsAaQWKYt9VRd4li8i+3UQXGLPSPr3FbV:SNp9CFEa4RMjFhThyaJj+N66z3F8+sW
TLSH:	51F42226BB93C772D90595B050B3051183F5D38A7637CA5B2D98A2DB0E673A0FF4AB4C
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....w7.....0..... ....@..... ....`...@.....@..... .....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
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:	0xB53777FE [Wed May 5 18:54:54 2066 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:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
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	0xc0000	0x598	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbebd4	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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text

Sections

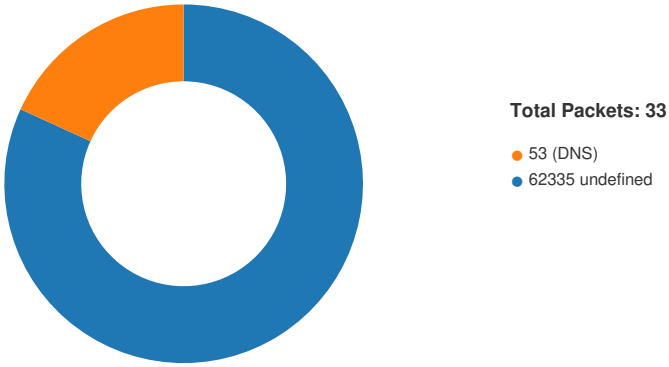
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbcc20	0xbce00	False	0.9689594018861681	data	7.967009459127166	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x598	0x600	False	0.412109375	data	4.066824834379209	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc00a0	0x30c	data		
RT_MANIFEST	0xc03ac	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 17:41:29.846982956 CEST	49693	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:41:32.860028028 CEST	49693	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:41:38.861643076 CEST	49693	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:41:49.086462975 CEST	49711	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:41:52.096015930 CEST	49711	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:41:58.112176895 CEST	49711	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:42:07.524621010 CEST	49712	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:42:10.535191059 CEST	49712	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:42:16.535546064 CEST	49712	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:42:26.428272009 CEST	49713	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:26.473097086 CEST	62335	49713	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:26.974164963 CEST	49713	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:27.020880938 CEST	62335	49713	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:27.536618948 CEST	49713	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:27.581342936 CEST	62335	49713	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:31.600708008 CEST	49714	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:31.645589113 CEST	62335	49714	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:32.146420002 CEST	49714	62335	192.168.2.5	91.193.75.178

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 17:42:32.191236973 CEST	62335	49714	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:32.693353891 CEST	49714	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:32.738332987 CEST	62335	49714	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:36.741517067 CEST	49715	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:36.786386013 CEST	62335	49715	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:37.287365913 CEST	49715	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:37.332129002 CEST	62335	49715	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:37.849920034 CEST	49715	62335	192.168.2.5	91.193.75.178
Jun 4, 2023 17:42:37.897248030 CEST	62335	49715	91.193.75.178	192.168.2.5
Jun 4, 2023 17:42:41.953573942 CEST	49716	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:42:44.962184906 CEST	49716	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:42:50.973063946 CEST	49716	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:43:01.282201052 CEST	49718	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:43:04.286673069 CEST	49718	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:43:10.287220001 CEST	49718	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:43:19.976326942 CEST	49719	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:43:22.975980997 CEST	49719	62335	192.168.2.5	102.90.46.28
Jun 4, 2023 17:43:28.980907917 CEST	49719	62335	192.168.2.5	102.90.46.28

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 17:41:29.799606085 CEST	50295	53	192.168.2.5	8.8.8.8
Jun 4, 2023 17:41:29.835984945 CEST	53	50295	8.8.8.8	192.168.2.5
Jun 4, 2023 17:41:49.048280001 CEST	49177	53	192.168.2.5	8.8.8.8
Jun 4, 2023 17:41:49.084583044 CEST	53	49177	8.8.8.8	192.168.2.5
Jun 4, 2023 17:42:07.508359909 CEST	49724	53	192.168.2.5	8.8.8.8
Jun 4, 2023 17:42:07.523355007 CEST	53	49724	8.8.8.8	192.168.2.5
Jun 4, 2023 17:42:41.917318106 CEST	61452	53	192.168.2.5	8.8.8.8
Jun 4, 2023 17:42:41.952620983 CEST	53	61452	8.8.8.8	192.168.2.5
Jun 4, 2023 17:43:01.252048016 CEST	51484	53	192.168.2.5	8.8.8.8
Jun 4, 2023 17:43:01.280893087 CEST	53	51484	8.8.8.8	192.168.2.5
Jun 4, 2023 17:43:19.947905064 CEST	63446	53	192.168.2.5	8.8.8.8
Jun 4, 2023 17:43:19.974457026 CEST	53	63446	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 4, 2023 17:41:29.799606085 CEST	192.168.2.5	8.8.8.8	0x6fb5	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:41:49.048280001 CEST	192.168.2.5	8.8.8.8	0x3885	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:42:07.508359909 CEST	192.168.2.5	8.8.8.8	0xe889	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:42:41.917318106 CEST	192.168.2.5	8.8.8.8	0xe4a3	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:43:01.252048016 CEST	192.168.2.5	8.8.8.8	0x9bda	Standard query (0)	ezemnia3.ddns.net	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:43:19.947905064 CEST	192.168.2.5	8.8.8.8	0x4553	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 4, 2023 17:41:29.835984945 CEST	8.8.8.8	192.168.2.5	0x6fb5	No error (0)	ezemnia3.ddns.net		102.90.46.28	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:41:49.084583044 CEST	8.8.8.8	192.168.2.5	0x3885	No error (0)	ezemnia3.ddns.net		102.90.46.28	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:42:07.523355007 CEST	8.8.8.8	192.168.2.5	0xe889	No error (0)	ezemnia3.ddns.net		102.90.46.28	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 4, 2023 17:42:41.952620983 CEST	8.8.8.8	192.168.2.5	0xe4a3	No error (0)	ezemnia3.ddns.net		102.90.46.28	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:43:01.280893087 CEST	8.8.8.8	192.168.2.5	0x9bda	No error (0)	ezemnia3.ddns.net		102.90.46.28	A (IP address)	IN (0x0001)	false
Jun 4, 2023 17:43:19.974457026 CEST	8.8.8.8	192.168.2.5	0x4553	No error (0)	ezemnia3.ddns.net		102.90.46.28	A (IP address)	IN (0x0001)	false

Statistics

Behavior

System Behavior

Analysis Process: NA.exe PID: **1544**, Parent PID: **3324**

General

Target ID:	0
Start time:	17:41:24
Start date:	04/06/2023
Path:	C:\Users\user\Desktop\NA.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\NA.exe
Imagebase:	0x161787e0000
File size:	775680 bytes
MD5 hash:	6C432A8B26BC0E068F23E88F69C0F565
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: 00000000.00000002.387169472.0000016110009000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.387169472.0000016110009000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.387169472.0000016110009000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.387169472.0000016110009000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.387169472.0000016110167000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.387169472.0000016110167000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.387169472.0000016110167000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.387169472.0000016110167000.00000004.00000800.00020000.00000000.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\NA.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA055886ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\NA.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	7FFA05588769	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	7FFA04FEB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA04FEB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA050C12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04FF2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA050C12E7	ReadFile

Analysis Process: CasPol.exe PID: **5528**, Parent PID: **1544**

General

Target ID:	1
Start time:	17:41:26

Start date:	04/06/2023
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:	0x7f0000
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: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.656680345.0000000005CE0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.650425425.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.650425425.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.650425425.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.650425425.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.656751098.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.656751098.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.656751098.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.656751098.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.656751098.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.654572107.0000000003E99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.654572107.0000000003E99000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.654572107.0000000003E99000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.651668667.0000000002E91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.651668667.0000000002E91000.00000004.00000800.00020000.00000000.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	7222CF06	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	7222CF06	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	7222CF06	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	7222CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7107BEFF	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	71071E60	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	7107BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7107DD66	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	7107BEFF	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	7107BEFF	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 2e 1b fd 5d 65 fd 48	.]eH	success or wait	1	71071B4F	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	7107DD66	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	4096	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	512	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72205705	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	7107646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **4584**, Parent PID: **3324**

General

Target ID:	4
Start time:	17:41:39
Start date:	04/06/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xc30000
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

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	7253C78D	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	71071B4F	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	71071B4F	WriteFile
\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	71071B4F	WriteFile
\Device\ConDrv	486	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71071B4F	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	7253C907	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile

Analysis Process: conhost.exe PID: **7148**, Parent PID: **4584**

General

Target ID:	5
Start time:	17:41:39
Start date:	04/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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