ID: 559032
Sample Name:
B3MC87V5_INV0ICE.exe
Cookbook: default.jbs
Time: 19:40:17
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

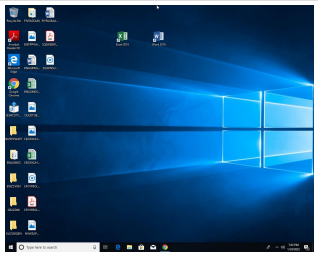
Windows Analysis Report

B3MC87V5_INV0ICE.exe

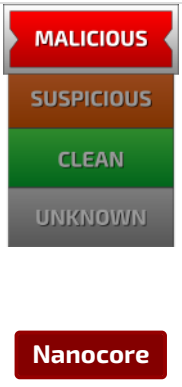
Overview

General Information

Sample Name:	B3MC87V5_INV0ICE.exe
Analysis ID:	559032
MD5:	a2b3eecc7775a0..
SHA1:	abee79039620ad.
SHA256:	368efd9a4c1735..
Infos:	



Detection



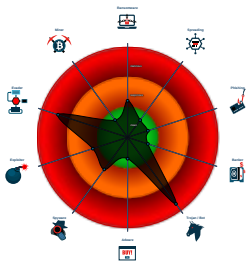
Nanocore

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

Signatures

- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to delay execution (extensive …
- .NET source code references suspic…
- Machine Learning detection for sam…
- Binary or sample is protected by do…
- Injects a PE file into a foreign proce…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- B3MC87V5_INV0ICE.exe (PID: 5964 cmdline: "C:\Users\user\Desktop\B3MC87V5_INV0ICE.exe" MD5: A2B3EECC7775A0DAD0BED6CA51ED33C9)
  - RegAsm.exe (PID: 6532 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - cmd.exe (PID: 1860 cmdline: cmd" /c mkdir "C:\Users\user\AppData\Roaming\haygsed MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6004 cmdline: "cmd" /c schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\haygsed\haygsed.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5884 cmdline: schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\haygsed\haygsed.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 6012 cmdline: cmd" /c copy "C:\Users\user\Desktop\B3MC87V5_INV0ICE.exe" "C:\Users\user\AppData\Roaming\haygsed\haygsed.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- haygsed.exe (PID: 6368 cmdline: C:\Users\user\AppData\Roaming\haygsed\haygsed.exe MD5: A2B3EECC7775A0DAD0BED6CA51ED33C9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.566252291.0000000000702000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000004.00000002.566252291.0000000000702000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.566252291.0000000000702000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000004.00000000.378815148.0000000000702000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000000.378815148.0000000000702000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 55 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.RegAsm.exe.6b20000.33.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
4.2.RegAsm.exe.6b20000.33.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
4.2.RegAsm.exe.3b1aa5f.14.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
4.2.RegAsm.exe.3b1aa5f.14.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
4.2.RegAsm.exe.58e0000.22.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 160 entries				

Sigma Overview

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

System Summary

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Jbx Signature Overview

AV Detection

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Binary or sample is protected by dotNetProtector

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Tries to delay execution (extensive OutputDebugStringW loop)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

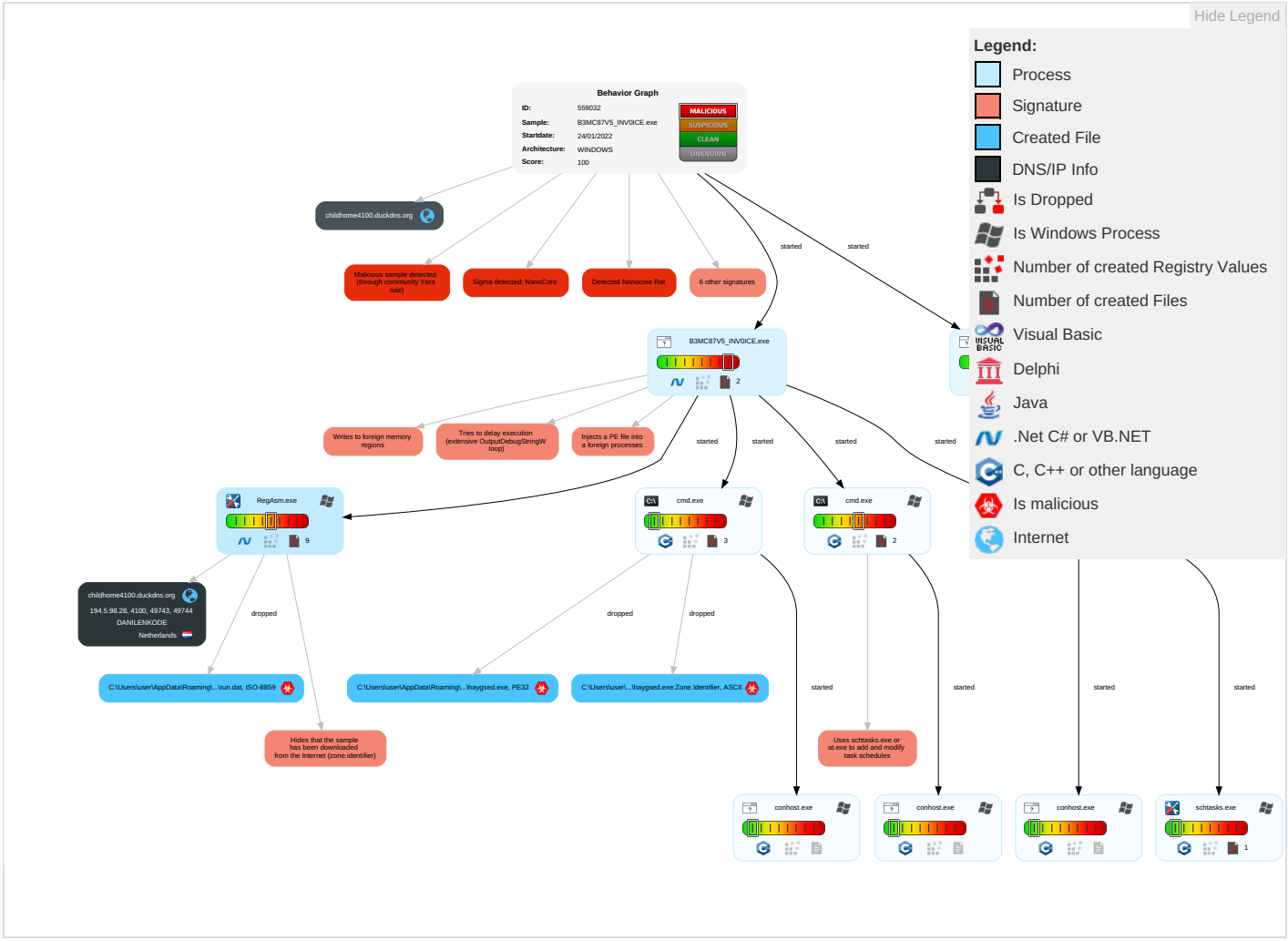
Remote Access Functionality

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	2 Windows Management Instrumentation	1 Scheduled Task/Job	2 1 2 Process Injection	1 Masquerading	1 1 Input Capture	1 System Time 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	1 Scheduled Task/Job	1 DLL Side-Loading	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	3 1 Security Software 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	1 Native API	Logon Script (Windows)	1 DLL Side-Loading	1 4 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 2 Process Injection	NTDS	1 4 1 Virtualization/Sandbox Evasion	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 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	2 3 System Information 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 1 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	1 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 DLL Side-Loading	/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
B3MC87V5_INV0ICE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\haygsed\haygsed.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.RegAsm.exe.58e0000.22.unpack	100%	Avira	TR/NanoCore.fadte		Download File
4.2.RegAsm.exe.700000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.RegAsm.exe.700000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.RegAsm.exe.700000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.RegAsm.exe.700000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.RegAsm.exe.700000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.RegAsm.exe.3778a48.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
4.0.RegAsm.exe.700000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
childhome4100.duckdns.org	194.5.98.28	true	false		high

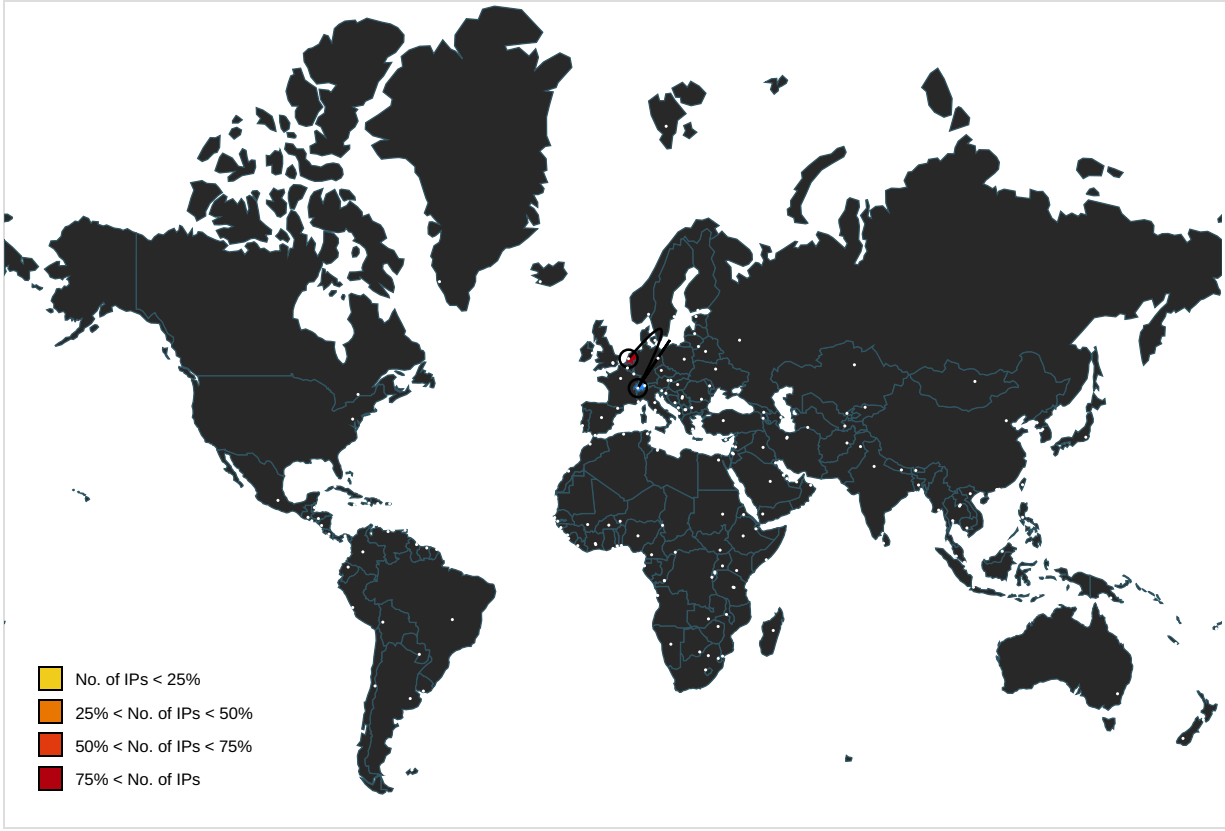
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
0,0,296364674,0000000000A75000,00000104,00000010,00020000,00000000,1,0	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	RegAsm.exe, 00000004.00000002.571486286.0000000003A88000.00000004.00000800.00020000.00000000.sdmp, RegAsm.exe, 00000004.00000002.571679195.0000000003B92000.00000004.00000800.00020000.00000000.sdmp, RegAsm.exe, 00000004.00000002.573635618.00000000006660000.00000004.08000000.00040000.00000000.sdmp, RegAsm.exe, 00000004.00000002.570614946.00000000037E2000.00000004.00000800.00020000.00000000.sdmp, RegAsm.exe, 00000004.00000002.568040726.0000000002783000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegAsm.exe, 00000004.00000002.567864641.0000000002711000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.28	childhome4100.duckdns.org	Netherlands		208476	DANILENKODE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	559032
Start date:	24.01.2022
Start time:	19:40:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	B3MC87V5_INV0ICE.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/6@12/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:41:27	API Interceptor	1x Sleep call for process: B3MC87V5_INV0ICE.exe modified
19:42:00	Task Scheduler	Run new task: Nanias path: "C:\Users\user\AppData\Roaming\haygsed\haygsed.exe"
19:42:02	API Interceptor	690x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408

Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:uD8tn:ugt
MD5:	39781087EE23D0146F9ED7FBAE34A487
SHA1:	30E0C05BF82927EF6A672D96B4D1E7FE2933EEA5
SHA-256:	32DF9A7851E650AFD0BF92304C6CAE51B4CF5C50C969A74DF5685DFB1FB2B2DD
SHA-512:	20F0D585ED872D0325D0970CC9C9C169C65A38D3893BBBF6DF60F7282D4A81817CB55221583B885B5AFB5C9DAFE4BE70B3916B36310A8EAB9D300E096FCCCF5
Malicious:	**true**
Reputation:	unknown
Preview:	.....H

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999475200956989**
Encrypted:	**true**
SSDEEP:	6144:Lg7wA4ZGTWZuVQkLrY9ibkRCi4ysdhYfAZuOGwJ:u4EKgVvtbpi4ysdhYfAERe
MD5:	3C0C5B80A03916CAD785A3F894BE46DE
SHA1:	ED60C66D695EECF3E001ECC364AE7D07591399E1
SHA-256:	B38D9BFED150EA6247C524D0563A41370324FF6EB2D8B393690EDF0BD822CE27
SHA-512:	A77D28488612F2AF9AD4B1A80FB2A542BE52BF377A0A4D8955FD5DC562680C6CD01FE221410E4B646BA4ED6A1F284E2151AC88C462E11AC6109B0DFF8FB3ECC7
Malicious:	false

Reputation:	unknown
Preview:	.6+N.....M.*....[.....+T.@=..Yx.!FMl...r0.7....g....g(..L..(c.*..H.....gGv.VQ.K..'.P...j0.....R...3$8l.}".t.N$G.1R.a..cH.fW..|.A1.!..e.W...c...`.B?D...;.e`Y.6.1]~.69.Qc..<..S.Ws:..T.....1X..D...`.~..Z..J...`}j..0.....b.N..Z...{.....9....i/K..x.{l.'|J...{.E..J6.l.....Vh..a.{Y.*W...._o..m.Ud`p.J...,.A...Oo...3...E.p..#....ii..8c.";..[Q....AYFk.v..=...U%.:.\...3..jP...o.....:Jw.]t...5.....B.O[.M$tj....=.b.Q.0.....r...J.kN..t't]....Q.....V...G^.D-...4@I.W7...[.....l\..#'.,..ek6.c..M.....d.L.>r`..u&{...e.ND.~.....>..Ct.j.trh..o.UG".....J....T..T...z.>.....o.....K.j..O...A...e.....%.$.Ap..W.....(.`....6..|..7.k.,....f.....s..F... 1..7.8..k..JE.....au._...3.axk...T1.Z../x.+...p.r&E.G.....).w;.]...P..J.j.....(.4...r..D.....B..^K4no.(..G....wA..%(KW*.?.w.N.'A..`.....[..i{._.._/yM.p.A.4..^.RI..q..T....P..&g5e.ykB....(..L..C+.Nx0...A%.1.C.m..RV..^....'.{..S?....t....>u6V&.&7..F%.....+?

C:\Users\user\AppData\Roaming\haygsed\haygsed.exe

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	314572800
Entropy (8bit):	0.026306809612278496
Encrypted:	false
SSDEEP:	6144:8Lz9vCIlX0Q6UNJA0zmajAInRsPZZR7go7ssKin6jMEtEbjMj5J8iP1:8LVzl40zz+WRqRccslY6xJV/
MD5:	A2B3EECC7775A0DAD0BED6CA51ED33C9
SHA1:	ABEE79039620AD209EBE02DAB2A11FD2AC2F24A6
SHA-256:	368EFD9A4C1735F889EC21D74AC599636A1D5846602629DC6ADAFB1A91035630
SHA-512:	596F0AFCEAC09C7543D480064D6A3030310ED2087658DCBCEBA021B5AF239F54567C7D937286E392DFEFF4D408D692B048F5E8EB94ABB26D38BA4AD921C459A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$..a.....F..... ... .@.. ....@.....K.... ...B..... ....H.....text..... ....`.rsrc....B... ...D.....@..@.rel oc.....B.....@..B.....H.....T]...,.....L...t2...*.....~&...(....z..(....*..-.*(....&*..(....*.*^~(....(....~)....(....*2~.....(....*..{....*..{....*:~.....(... .*..{....*..{....*:~.....(....*..{....*6~.....(....*..{....*..{....*..{....*..{....*..{....*..{....*.~....(....*..{....*..{....*.~....(....*..{....*.~'...(....*..{....*..{....*..0.....#.....@#.....U@[(x...(..... .#.....X@#.....H@(y...X(x...($.....#.....X@#.....@@Y(x...(..

C:\Users\user\AppData\Roaming\haygsed\haygsed.exe:Zone.Identifier

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	0.026306809612278496
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	B3MC87V5_INV0ICE.exe
File size:	314572800
MD5:	a2b3eecc7775a0dad0bed6ca51ed33c9
SHA1:	abee79039620ad209ebe02dab2a11fd2ac2f24a6
SHA256:	368efd9a4c1735f889ec21d74ac599636a1d5846602629dc6adafb1a91035630

SHA512:	596f0afceac09c7543d480064d6a3030310ed2087658dcbceba021b5af239f54567c7d937286e392dfeff4d408d692b048f5e8eb94abb26d38ba4ad921c4593a
SSDEEP:	6144:8Lz9vCIlX0Q6UNJA0zmajAInRsPZZR7go7ssKin6jMEtEbjMj5J8iP1:8LVzl40zz+WRqRccslY6xJV/
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...$..a.....................F........... ... .@.. .... @................................

File Icon

Icon Hash:	b270f086c6c2caf0

Static PE Info

General

Entrypoint:	0x471bce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61EAB124 [Fri Jan 21 13:12:04 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x71b80	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x72000	0x242ee	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x98000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6fbd4	0x6fc00	False	0.62571439807	data	6.77389980886	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x72000	0x242ee	0x24400	False	0.157388200431	data	3.5291437187	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x98000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
EDPENLIGHTENEDAPPINFOID	0x72568	0x2	data		
EDPPERMISSIVEAPPINFOID	0x7256c	0x2	data		
GOOGLEUPDATEAPPLICATIONCOMMANDS	0x72570	0x4	data		
RT_CURSOR	0x72574	0x134	data		
RT_CURSOR	0x726a8	0xb4	data		
RT_ICON	0x7275c	0x1d4f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x744ac	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x84cd4	0x94a8	data		
RT_ICON	0x8e17c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4043309055, next used block 4294967047		
RT_ICON	0x923a4	0x25a8	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9494c	0x10a8	data		
RT_ICON	0x959f4	0x468	GLS_BINARY_LSB_FIRST		
RT_RCDATA	0x95e5c	0x10	data		
RT_GROUP_CURSOR	0x95e6c	0x22	Lotus unknown worksheet or configuration, revision 0x2		
RT_GROUP_ICON	0x95e90	0x68	data		
RT_VERSION	0x95ef8	0x20c	data		
RT_MANIFEST	0x96104	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Frnkknk
FileVersion	5, 6, 0, 1
CompanyName	bokoihFmm
ProductName	
ProductVersion	5, 6, 0, 1
FileDescription	en
Translation	0x0409 0x04b0

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/22-19:42:05.133842	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57459	8.8.8.8	192.168.2.3
01/24/22-19:42:11.771249	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57875	8.8.8.8	192.168.2.3
01/24/22-19:42:18.902291	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54154	8.8.8.8	192.168.2.3
01/24/22-19:42:25.934060	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
01/24/22-19:42:32.324106	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.3
01/24/22-19:42:47.442400	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56527	8.8.8.8	192.168.2.3
01/24/22-19:42:55.157171	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49559	8.8.8.8	192.168.2.3
01/24/22-19:43:16.672224	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58361	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 19:42:05.226300955 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:05.439652920 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:05.439856052 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:05.828263998 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:06.071022987 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:06.071288109 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:06.326030970 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:06.326188087 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:06.541294098 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:06.541873932 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:06.798820972 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:06.798928976 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.061203003 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.091367960 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.091444969 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.091516018 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.092108965 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.092799902 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.092925072 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.305099964 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.305367947 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.305516005 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.305541992 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.305697918 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.305761099 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.306591988 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.306647062 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.306699991 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.306718111 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.306876898 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.306938887 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.519232988 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.519272089 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.519293070 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.519370079 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.519558907 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.519632101 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.520039082 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.520191908 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.520283937 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.520339012 CET	4100	49743	194.5.98.28	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 19:42:07.520562887 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.520621061 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.520668030 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.520808935 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.520875931 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.521354914 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.521378994 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.521476984 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.521492004 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.521516085 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.521537066 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.521559954 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.521572113 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.521615028 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.527954102 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.736143112 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736181974 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736198902 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736216068 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736232042 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736244917 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.736248016 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736267090 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736279011 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.736287117 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736294031 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.736304998 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736321926 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736330032 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.736344099 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736357927 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.736368895 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.736392021 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.736418009 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738007069 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738030910 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738046885 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738063097 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738117933 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738126040 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738140106 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738143921 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738157034 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738163948 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738179922 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738203049 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738214970 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738224983 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738226891 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738262892 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738266945 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738280058 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738285065 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738301992 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738322020 CET	49743	4100	192.168.2.3	194.5.98.28
Jan 24, 2022 19:42:07.738645077 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738670111 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738691092 CET	4100	49743	194.5.98.28	192.168.2.3
Jan 24, 2022 19:42:07.738713026 CET	4100	49743	194.5.98.28	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 19:42:05.025234938 CET	57459	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:05.133841991 CET	53	57459	8.8.8.8	192.168.2.3
Jan 24, 2022 19:42:11.663330078 CET	57875	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:11.771249056 CET	53	57875	8.8.8.8	192.168.2.3
Jan 24, 2022 19:42:18.793790102 CET	54154	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:18.902291059 CET	53	54154	8.8.8.8	192.168.2.3
Jan 24, 2022 19:42:25.824975014 CET	52806	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:25.934060097 CET	53	52806	8.8.8.8	192.168.2.3
Jan 24, 2022 19:42:32.214613914 CET	64021	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:32.324105978 CET	53	64021	8.8.8.8	192.168.2.3
Jan 24, 2022 19:42:39.378787041 CET	52130	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:39.398076057 CET	53	52130	8.8.8.8	192.168.2.3
Jan 24, 2022 19:42:47.332921982 CET	56527	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:47.442399979 CET	53	56527	8.8.8.8	192.168.2.3
Jan 24, 2022 19:42:55.048990011 CET	49559	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:42:55.157171011 CET	53	49559	8.8.8.8	192.168.2.3
Jan 24, 2022 19:43:01.371299028 CET	52650	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:43:01.390882969 CET	53	52650	8.8.8.8	192.168.2.3
Jan 24, 2022 19:43:08.589274883 CET	63297	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:43:08.608269930 CET	53	63297	8.8.8.8	192.168.2.3
Jan 24, 2022 19:43:16.556576967 CET	58361	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:43:16.672224045 CET	53	58361	8.8.8.8	192.168.2.3
Jan 24, 2022 19:43:23.475601912 CET	53615	53	192.168.2.3	8.8.8.8
Jan 24, 2022 19:43:23.494785070 CET	53	53615	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2022 19:42:05.025234938 CET	192.168.2.3	8.8.8.8	0x786	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:11.663330078 CET	192.168.2.3	8.8.8.8	0x687	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:18.793790102 CET	192.168.2.3	8.8.8.8	0xb4e2	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:25.824975014 CET	192.168.2.3	8.8.8.8	0x7b57	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:32.214613914 CET	192.168.2.3	8.8.8.8	0x37d8	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:39.378787041 CET	192.168.2.3	8.8.8.8	0x8e63	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:47.332921982 CET	192.168.2.3	8.8.8.8	0xc07f	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:55.048990011 CET	192.168.2.3	8.8.8.8	0x778	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:01.371299028 CET	192.168.2.3	8.8.8.8	0xcaf5	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:08.589274883 CET	192.168.2.3	8.8.8.8	0xee43	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:16.556576967 CET	192.168.2.3	8.8.8.8	0x905c	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:23.475601912 CET	192.168.2.3	8.8.8.8	0x5c96	Standard query (0)	childhome4 100.duckdns.org	A (IP address)	IN (0x0001)

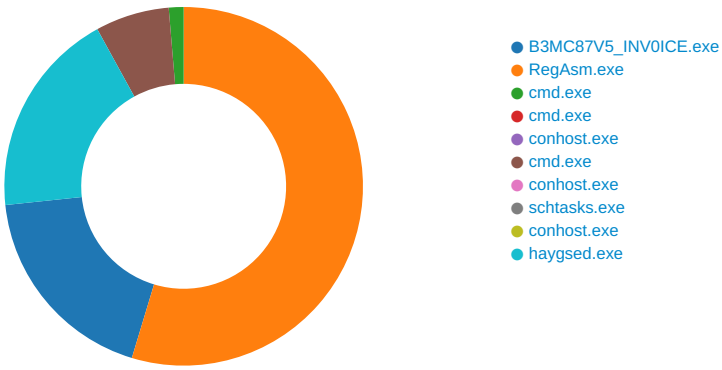
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 19:42:05.133841991 CET	8.8.8.8	192.168.2.3	0x786	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:11.771249056 CET	8.8.8.8	192.168.2.3	0x687	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:18.902291059 CET	8.8.8.8	192.168.2.3	0xb4e2	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 19:42:25.934060097 CET	8.8.8.8	192.168.2.3	0x7b57	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:32.324105978 CET	8.8.8.8	192.168.2.3	0x37d8	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:39.398076057 CET	8.8.8.8	192.168.2.3	0x8e63	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:47.442399979 CET	8.8.8.8	192.168.2.3	0xc07f	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:42:55.157171011 CET	8.8.8.8	192.168.2.3	0x778	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:01.390882969 CET	8.8.8.8	192.168.2.3	0xcaf5	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:08.608269930 CET	8.8.8.8	192.168.2.3	0xee43	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:16.672224045 CET	8.8.8.8	192.168.2.3	0x905c	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 24, 2022 19:43:23.494785070 CET	8.8.8.8	192.168.2.3	0x5c96	No error (0)	childhome4 100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: B3MC87V5_INV0ICE.exe PID: **5964**, Parent PID: **4776**

General

Start time:	19:41:16
Start date:	24/01/2022
Path:	C:\Users\user\Desktop\B3MC87V5_INV0ICE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\B3MC87V5_INV0ICE.exe"
Imagebase:	0x1190000
File size:	314572800 bytes
MD5 hash:	A2B3EECC7775A0DAD0BED6CA51ED33C9
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: 00000000.00000002.568236668.0000000003C3A000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.568236668.0000000003C3A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.568236668.0000000003C3A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Analysis Process: RegAsm.exe PID: **6532**, Parent PID: **5964**

General

Start time:	19:41:54
Start date:	24/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x320000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000004.00000002.566252291.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.566252291.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.566252291.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.378815148.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.378815148.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.378815148.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573531142.0000000006610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573531142.0000000006610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.571486286.0000000003A88000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.571679195.0000000003B92000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.571679195.0000000003B92000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573665805.0000000006670000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573665805.0000000006670000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.572572117.0000000005040000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.572572117.0000000005040000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573911578.000000006B70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573911578.000000006B70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573600935.0000000006640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573600935.0000000006640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573635618.0000000006660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573635618.0000000006660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573808186.000000006B00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573808186.000000006B00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573456307.0000000006590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573456307.0000000006590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573579874.0000000006630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573579874.0000000006630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.379092491.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.379092491.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.379092491.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573857285.0000000006B20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573857285.0000000006B20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.570437882.0000000003761000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573871783.0000000006B30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573871783.0000000006B30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.379340536.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.379340536.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.379340536.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573474368.00000000065A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573474368.00000000065A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.567864641.0000000002711000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.570614946.00000000037E2000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.573618982.0000000006650000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.573618982.0000000006650000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.379594282.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.379594282.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.379594282.0000000000702000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.572722744.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.572722744.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.572722744.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.568040726.0000000002783000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

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	6E86CF06	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	6E86CF06	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	6D6BBEFF	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	6D6B1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D6BBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D6BBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	9	6D6B1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D6B1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D6B1E60	CreateFileW

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	20 fd e5 fd fd fd 48	H	success or wait	1	6D6B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	11	6D6B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327768	fd 36 2b 4e fd fd fd fd fd 1e 91 fd 10 4d 12 2a 1d fd 0f 06 5b fd fd fd 05 17 2b 54 fd 40 3d fd 7f 59 78 fd 21 46 4d 6c 12 b1 fd 72 30 f8 37 fd fd 09 15 67 b4 fd fd 13 67 28 fd fd 4c 17 fd 28 63 fd 2a fd fd 48 fd fd fd 1f 18 fd 67 47 76 18 56 51 fd 4b fd 07 27 fd 50 fd fd fd 6a 30 fd 0b fd 14 fd fd fd fd fd 52 1f 02 fd 33 24 38 6c fd 7d 22 fd 74 fd 4e 24 47 fd 31 52 fd 61 07 fd 63 48 fd 66 57 fd 0d 7c 1b 41 31 fd 21 fd fd 65 fd 57 03 fd fd 63 fd fd fd 60 fd 42 3f 44 fd 09 fd 3b fd 65 60 59 01 36 fd 31 5d 7e fd 36 39 fd 51 63 fd fd 3c fd fd 53 99 57 73 3a fd fd 54 fd 06 fd fd c6 1c 1b fd 31 58 fd 1f 44 00 fd fd 60 fd 7e fd fd 5a fd c4 4a fd fd fd 60 7d 6a fd fd 30 fd 09 fd fd fd fd 16 fd fd fd fd fd fd fd 62 fd 4e	6+NM* [+T@=Yx!FMlr07gg(L(c* HgGv VQK'Pj0R3$8l}"tN$G1Ra cHfW|A1!eWc`B? D;e`Y61]~69Qc<SWs:T1 XD`~ZJ`}j0bN	success or wait	1	6D6B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6D6B1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E845705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6E84CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6E84CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E84CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6E7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6D6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6D6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	4096	success or wait	1	6E82D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	512	success or wait	1	6E82D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6E845705	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6E82D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6E82D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E82D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E82D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	2	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6E845705	unknown

Analysis Process: cmd.exe PID: **1860**, Parent PID: **5964**

General

Start time:	19:41:57
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c mkdir "C:\Users\user\AppData\Roaming\haygsed
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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\Roaming\haygsed	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	D8BFE7	CreateDirectoryW

Analysis Process: cmd.exe PID: **6004**, Parent PID: **5964**

General

Start time:	19:41:58
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\haygsed\haygsed.exe'" /f
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6148**, Parent PID: **1860**

General

Start time:	19:41:58
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **6012**, Parent PID: **5964**

General

Start time:	19:41:59
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c copy "C:\Users\user\Desktop\B3MC87V5_INV0ICE.exe" "C:\Users\user\AppData\Roaming\haygsed\haygsed.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\haygsed\haygsed.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	D84E97	CopyFileExW
C:\Users\user\AppData\Roaming\haygsed\haygsed.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	D84E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\haygsed\haygsed.exe	0	1048576	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 24 fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 fd 06 00 00 46 02 00 00 00 00 00 fd 1b 07 00 00 20 00 00 00 20 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 09 00 00 02 00 00 fd fd 09 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.PELaF @ @	success or wait	300	D84E97	CopyFileExW
C:\Users\user\AppData\Roaming\haygsed\haygsed.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	D84E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B3MC87V5_INV0ICE.exe	unknown	512	success or wait	1	D85742	ReadFile

Analysis Process: conhost.exe PID: **5956**, Parent PID: **6004**

General

Start time:	19:41:59
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5884**, Parent PID: **6004**

General

Start time:	19:42:00
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\haygsed\haygsed.exe'" /f
Imagebase:	0xd0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4868**, Parent PID: **6012**

General

Start time:	19:42:00
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: haygsed.exe PID: **6368**, Parent PID: **664**

General

Start time:	19:43:03
Start date:	24/01/2022
Path:	C:\Users\user\AppData\Roaming\haygsed\haygsed.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\haygsed\haygsed.exe
Imagebase:	0x13b0000
File size:	314572800 bytes
MD5 hash:	A2B3EECC7775A0DAD0BED6CA51ED33C9
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

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	6E86CF06	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	6E86CF06	unknown

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	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E845705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E84CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E7A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E7A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E845705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D6B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D6B1B4F	ReadFile

Disassembly

No disassembly