ID: 552947
Sample Name: filedata
Cookbook: default.jbs
Time: 23:28:59
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

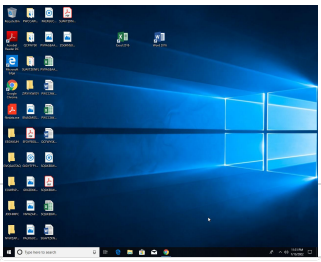
Windows Analysis Report filedata

Overview

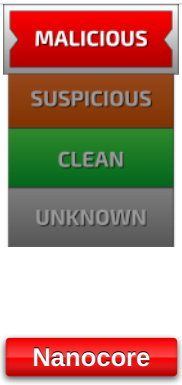
General Information

Sample Name:	filedata (renamed file extension from none to exe)
Analysis ID:	552947
MD5:	2ce21c68e4d03f3..
SHA1:	5963d9d448d322..
SHA256:	93d545c83fa4620.
Infos:	

Most interesting Screenshot:



Detection



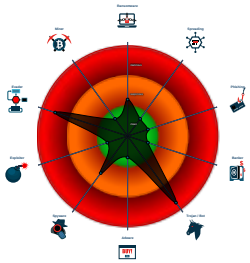
Nanocore

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Detected unpacking (creates a PE fi…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Uses dynamic DNS services
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…

Classification



Process Tree

- **System is w10x64**
- filedata.exe (PID: 6760 cmdline: "C:\Users\user\Desktop\filedata.exe" MD5: 2CE21C68E4D03F35248689663DC820DE)
  - filedata.exe (PID: 6220 cmdline: "C:\Users\user\Desktop\filedata.exe" MD5: 2CE21C68E4D03F35248689663DC820DE)
- chmac.exe (PID: 2812 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: 2CE21C68E4D03F35248689663DC820DE)
  - chmac.exe (PID: 6352 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: 2CE21C68E4D03F35248689663DC820DE)
- chmac.exe (PID: 4476 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: 2CE21C68E4D03F35248689663DC820DE)
  - chmac.exe (PID: 6968 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: 2CE21C68E4D03F35248689663DC820DE)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.361160585.000000000492 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000002.361160585.000000000492 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0000000B.00000002.361160585.000000000492 0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.361160585.000000000492 0000.00000004.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
00000005.00000000.298557071.000000000041 4000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x111e5:$x1: NanoCore.ClientPluginHost • 0x11222:$x2: IClientNetworkHost • 0x14d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 144 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.filedata.exe.5370000.34.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
5.2.filedata.exe.5370000.34.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
5.2.filedata.exe.383df59.19.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x7eb2e:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x7eb48:$x2: IClientNetworkHost
5.2.filedata.exe.383df59.19.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x7eb2e:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x7fb63:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x7eb1b:$s5: IClientLoggingHost
5.2.filedata.exe.383df59.19.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 526 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Nanocore RAT

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Networking:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

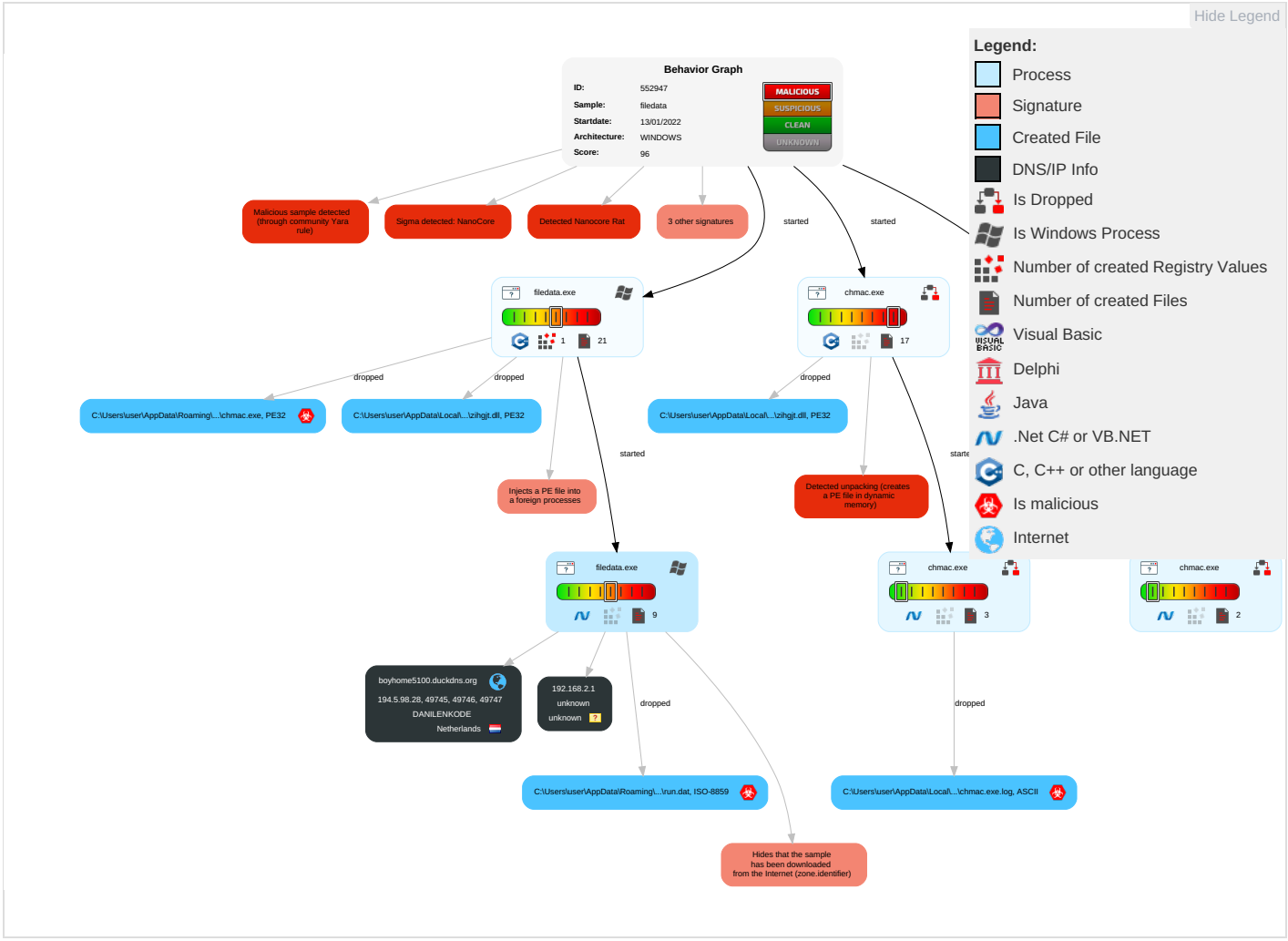
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdr Insecure Network Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Standard Port 1	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	System Information Discovery 1 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 1	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

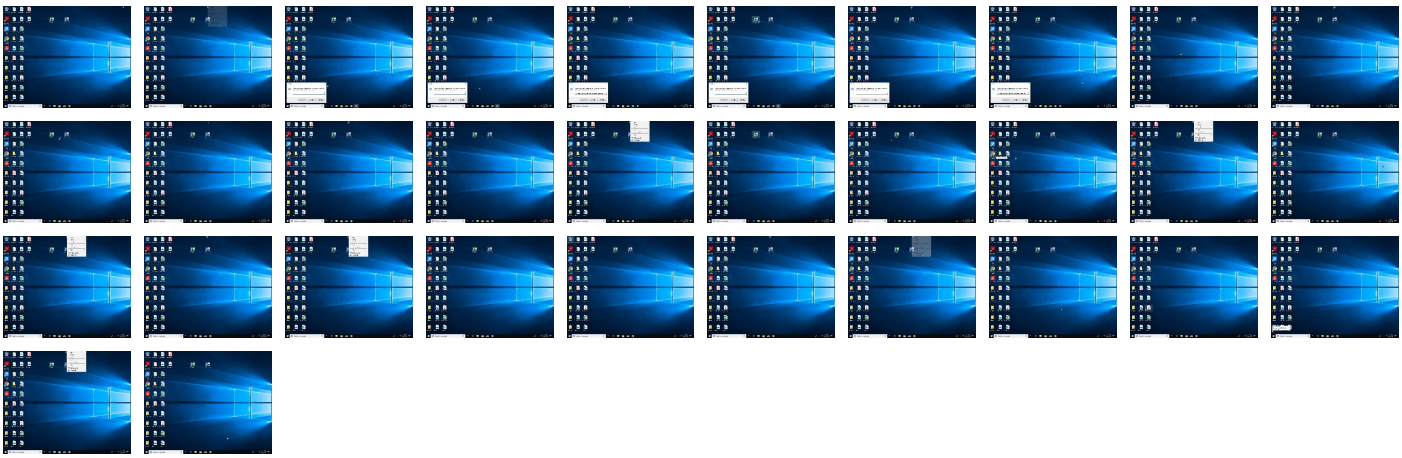
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.filedata.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.filedata.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.1.chmac.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.filedata.exe.4bc0000.32.unpack	100%	Avira	TR/NanoCore.fadte		Download File
11.0.chmac.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.chmac.exe.4810000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.1.chmac.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.chmac.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.chmac.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.filedata.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.chmac.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.chmac.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.filedata.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
8.2.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.chmac.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.chmac.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.filedata.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.chmac.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.filedata.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.filedata.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.filedata.exe.23f0000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.chmac.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.chmac.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.chmac.exe.4960000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.filedata.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.chmac.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.1.filedata.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.filedata.exe.3220000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.2.chmac.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.chmac.exe.400000.3.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
boyhome5100.duckdns.org	194.5.98.28	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.28	boyhome5100.duckdns.org	Netherlands		208476	DANILENKODE	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552947
Start date:	13.01.2022
Start time:	23:28:59
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 13m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	filedata (renamed file extension from none to 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:	25
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:	mal96.troj.evad.winEXE@9/13@19/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 29.1% (good quality ratio 26.8%) • Quality average: 73.9% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:29:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kyvrnrwl C:\Users\user\AppData\Roaming\dihsw\chmac.exe
23:30:00	API Interceptor	944x Sleep call for process: filedata.exe modified
23:30:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kyvrnrwl C:\Users\user\AppData\Roaming\dihsw\chmac.exe
23:30:05	API Interceptor	2x Sleep call for process: chmac.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\chmac.exe.log	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\671ojhadbggvsw	
Process:	C:\Users\user\Desktop\filedata.exe
File Type:	data
Category:	dropped
Size (bytes):	278527
Entropy (8bit):	7.987787031163242
Encrypted:	false
SSDEEP:	6144:JyjBoleNjaczUJPSzq5TmUoW6saM3urgNNbbHb1BCjyW9yRJt:JwCqeczMS+t2W606oZ5Y+t
MD5:	0037B7C03C75B524F1B5DA59BD0D97AF
SHA1:	A8162ADBB06CD85B408B19AAB1467344C0214EBC
SHA-256:	D08272389DCC58B662F32AA01F819E1B8C5C60FAC52224FB822123ABBB00D10E
SHA-512:	695B639051E2A4412515B160C61F718DA9436774658960A87C94E498C9A172B160DE11314E83239616203D95DA1B1BB2B92B5FE0D2A63A68CDBFC806673A8600
Malicious:	false
Reputation:	unknown
Preview:	/...+...F..+._d...6..%[$B..c.-.H.*.D}....P...N.....I.>..dp.|.~8.P..i.67..X.)8tU(J.T.R...~.G.?.R.*=.lgO...e....T8.`,..Q3yM.J._/....<..vn.>...?..,.....zn6b.....oj...I?a..(..j..K...w;.A.PFa.....jF..s,..,.....s.....\.....q...J."w..y..x.....5.,...r.+;._.....%[$...c+-...).D}0...FQ...N.q3...Y.>..dp.=,~6../..x.k`.M.9=...:.u....d.....t...({n./.....F.Z.3yM.J._...b#.+.HC.. .....>..M.<S.x.f.e...3*...\.8.V.-.({..2.S....0..o..pBkx.%.Gtz@.b.\x;...Q.X.W.....]...xX.q.n.#3...x.....q..@...i..+}.d.O.6...[$...c.-.H.*.D..V...;.`N.<....^.>..dp.I.~6../..x..`.M`9=....I...t.~...2.....p../.....".~C.'.J.._.....].@.C;.2.....\..M.<..xM...^..3*;b.\...V.4.(..[2.S....0..o..Bk..%.Gtz@..).\.;...Q.X.W..?...Q...xX.q.n.#3...x.....5.,.....+}.d.O.6..%[$...c.-.H.*.D}....P...N.....I.>..dp.=.~6../..x..`.M.9=.s.n.u.....~.....t...({../.....Z.3yM.J._...b#.@..C;. .....\..M.<S.x.f.e...3*...\.8.V.G.(...2.S....0..o..pBkx.%.Gtz@..).\.;...Q.X.W..?...Q..

C:\Users\user\AppData\Local\Temp\nsf55B6.tmp	
Process:	C:\Users\user\Desktop\filedata.exe
File Type:	data
Category:	dropped
Size (bytes):	509164
Entropy (8bit):	7.276677920260067
Encrypted:	false
SSDEEP:	12288:K1JwCqeczMS+t2W606oZ5Y+eHHGnCYFD6TG9pjni6v:KE1zcE+eHHGTACLv
MD5:	45C0D0E2E6C46774F79BC514DECDC37E
SHA1:	D2D3CAAFBE35107F7077D2122E9CFE6DD6353877
SHA-256:	FB58D337C61534E44945B4383FE380C86A20208114B34947C6FCD6E13348D0E8
SHA-512:	9269FC7A3D801884AF742252BF4829DE9DCBFB7A06CF4BE9DF86F0154F5BD9F2CEFE631C16C1652DF638942591E1C3016EE292C8C01637FFFC17CE9379D5091
Malicious:	false
Reputation:	unknown
Preview:	S_.....,.....DG.....m^.....;_..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsf55B7.tmp\zihgjt.dll	
Process:	C:\Users\user\Desktop\filedata.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.818353923098329
Encrypted:	false
SSDEEP:	6144:sUtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:snCYFD6TG9pjni6v
MD5:	83A517CDC6B25A8B9EEE20AD2AD4885D
SHA1:	7108BB963BA45544F7B3138329CA56EEB8DE86CC
SHA-256:	1F2B96F19BBB393643B033507D0B824321CABFFD596F991443999097B1031179
SHA-512:	60BF20CF9C4262E74F2B506A1D5F02A2977E625139118C2E694A52264A6ED2E0B552FD2ACFDC9B2A842813F5E028B5AFC052202633397780CDCAE03721DE9396
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...B...B...B.....B..C...B...C...B.a.F...B.a.B...B.d.....B.a.@...B.R ich..B.....PE..L...;G.a.....!.....@.....@..... .....0..x..... .....text...k..... ..`.rdata..2.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsi8283.tmp	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	data
Category:	dropped
Size (bytes):	509164
Entropy (8bit):	7.276677920260067
Encrypted:	false
SSDEEP:	12288:K1JwCqeczMS+t2W606oZ5Y+eHHGnCYFD6TG9pjni6v:KE1zcE+eHHGTACLv
MD5:	45C0D0E2E6C46774F79BC514DECDC37E
SHA1:	D2D3CAAFBE35107F7077D2122E9CFE6DD6353877
SHA-256:	FB58D337C61534E44945B4383FE380C86A20208114B34947C6FCD6E13348D0E8
SHA-512:	9269FC7A3D801884AF742252BF4829DE9DCBFB7A06CF4BE9DF86F0154F5BD9F2CEFE631C16C1652DF638942591E1C3016EE292C8C01637FFFC17CE9379D5091
Malicious:	false
Reputation:	unknown
Preview:	S_.....,.....DG.....m^.....;_..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsi8284.tmp\zihgjt.dll	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.818353923098329
Encrypted:	false
SSDEEP:	6144:sUtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:snCYFD6TG9pjni6v
MD5:	83A517CDC6B25A8B9EEE20AD2AD4885D
SHA1:	7108BB963BA45544F7B3138329CA56EEB8DE86CC
SHA-256:	1F2B96F19BBB393643B033507D0B824321CABFFD596F991443999097B1031179
SHA-512:	60BF20CF9C4262E74F2B506A1D5F02A2977E625139118C2E694A52264A6ED2E0B552FD2ACFDC9B2A842813F5E028B5AFC052202633397780CDCAE03721DE9396
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...B...B...B.....B..C...B...C...B.a.F...B.a.B...B.d.....B.a.@...B.R ich..B.....PE..L...;G.a.....!.....@.....@..... .....0..x..... .....text...k..... ..`.rdata..2.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsqA3A7.tmp	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	data
Category:	dropped
Size (bytes):	509164
Entropy (8bit):	7.276677920260067
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nsqA3A7.tmp	
SSDEEP:	12288:K1JwCqeczMS+t2W606oZ5Y+eHHGnCYFD6TG9pjni6v:KE1zcE+eHHGTACLv
MD5:	45C0D0E2E6C46774F79BC514DECDC37E
SHA1:	D2D3CAAFBE35107F7077D2122E9CFE6DD6353877
SHA-256:	FB58D337C61534E44945B4383FE380C86A20208114B34947C6FCD6E13348D0E8
SHA-512:	9269FC7A3D801884AF742252BF4829DE9DCBFB7A06CF4BE9DF86F0154F5BD9F2CEFE631C16C1652DF638942591E1C3016EE292C8C01637FFFC17CE9379D5091
Malicious:	false
Reputation:	unknown
Preview:	S_.....,.....DG.....m^.....;_..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsqA3A8.tmp\zihgjt.dll	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.818353923098329
Encrypted:	false
SSDEEP:	6144:sUtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:snCYFD6TG9pjni6v
MD5:	83A517CDC6B25A8B9EEE20AD2AD4885D
SHA1:	7108BB963BA45544F7B3138329CA56EEB8DE86CC
SHA-256:	1F2B96F19BBB393643B033507D0B824321CABFFD596F991443999097B1031179
SHA-512:	60BF20CF9C4262E74F2B506A1D5F02A2977E625139118C2E694A52264A6ED2E0B552FD2ACFDC9B2A842813F5E028B5AFC052202633397780CDCAE03721DE9396
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...B...B...B.....B..C...B...C...B.a.F...B.a.B...B.d.....B.a.@...B.R ich..B.....PE..L...;G.a.....!.....@.....@..... .....0..x..... .....text...k..... ..`.rdata..2.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\whpiswzko	
Process:	C:\Users\user\Desktop\filedata.exe
File Type:	data
Category:	dropped
Size (bytes):	7050
Entropy (8bit):	6.118390401908822
Encrypted:	false
SSDEEP:	192:QARpwFiGOPfrYJTdqMHrt5DDAnB96FUQCHQrRLhAKYoqA:+ifrejrU4AHIjAKY1A
MD5:	7FDBC0E9C2A4809011EBAF2722B58622
SHA1:	4B87C4B0BA5E681880FFAEDAC29744487DD3DDB2
SHA-256:	2B4D46A91010087F8B30D49470C9D0819ADF0F44EE1684C1CCA5F732CE2ACA62
SHA-512:	DEC7E80F10350A680FF316469FBFD2817B4937157082571AE4F859B837BA04489BC21B968C941B7769AF2CA07698B7111A9B748FA12EB5530367959FD96B08F0
Malicious:	false
Reputation:	unknown
Preview:	.t....C...L....).....&...I...&.....).....).....A.....E.tE.p.....A.....E.|E.x.....A....{...E..E.....A.....E..E.....R"..#.....5E.lE..C.....[.E..E..C..C..A..[z"....C.....A..E....E)...."[.....)... t...|....M....M...I....I...'.C..'.E.....tM.C...E...).....C)...C.....C.....C.....&....C..C.S....C..C.C..C..E..C...E..C..C.LC..E.C..C..C.....$.....$&.o..&.....$..3..... ....C.....&.....A.tE.....C.....C..LE..C...E.....I..C..5"..#..E..tE..pA..5"...m.E..tE..p"."..#..A..t.$&.o..}.....~...E....A.....E.....).....C..C.....C...L...&.....A..E.....C. ....C..LE..C...E.....I.HB...C..5"..#..E...E...C..5"...m.E...E...C..5"..}mE...E...C..[."..#z.E...E...A..5"...m.E...E...".".."..#..A....$.....k...E.....C..C..E.....W...E.....). .....C..C.....C.....A..E.....C.....C..LE..C...E....."...I..C..5"..#..E...E...C..5"...m.E...E...".".."..#..A...$..3.....E.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\filedata.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:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
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:\Users\user\Desktop\filedata.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:fJp8:fJp8
MD5:	9C9A932073E898A03B937105A5D91C30
SHA1:	3B53F50CF4EC7E40913CFBD2279E34E984CF309A
SHA-256:	3B4B7E29ADF8FF8CF49CDB924DE689CDB735A12EBD78DD29537E81A9454E9631
SHA-512:	C06CFE30E6DC392F0B9552685C3D47C190D5C308EB2B8BAEE4E60A9C1C25AF20B002A62EFC8911D70C828BE4C48818408C9E78C060BBC035400BEA76D14800F
Malicious:	**true**
Reputation:	unknown
Preview:	..I./..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\filedata.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Reputation:	unknown
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\dihsw\chmac.exe	
Process:	C:\Users\user\Desktop\filedata.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	784599
Entropy (8bit):	6.041735231045258
Encrypted:	false
SSDEEP:	6144:lwq9qYuoyUjNf5JXRf4RkwTxMiDWkFhvCZyHvV9unFgG9+RVB0qQVDK9gY2wZF+Z:oYuoLl5JRfO/dEyHbuqlt2wZbw
MD5:	2CE21C68E4D03F35248689663DC820DE
SHA1:	5963D9D448D322CB49F4DEE613734FE030131C11
SHA-256:	93D545C83FA462035AE0C2AA0036DB008FC4BDF3D10EC89C6F0B6699B09C6FBF
SHA-512:	2DD9A30D892FC0415976BDEB257658CFCC876A0B3935027E41E67D9272CC8DC3D4CCF882213DBA62653169AD159777CDF1E2866E98308FD05B78DF052437C12
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....p....@.....p.....s.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc.....t.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.041735231045258
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	filedata.exe
File size:	784599
MD5:	2ce21c68e4d03f35248689663dc820de
SHA1:	5963d9d448d322cb49f4dee613734fe030131c11
SHA256:	93d545c83fa462035ae0c2aa0036db008fc4bdf3d10ec89c6f0b6699b09c6fbf
SHA512:	2dd9a30d892fc0415976bdeb257658cfcc876a0b3935027e41e67d9272cc8dc3d4ccf882213dba62653169ad159777cdf1e2866e98308fd05b78df052437c122
SSDEEP:	6144:lwq9qYuoyUjNf5JXRf4RkwTxMiDWkFhvCZyHvV9unFgG9+RVB0qQVDK9gY2wZF+Z:oYuoLl5JRfO/dEyHbuqlt2wZbw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	d8c8d0d0f0ccd4d0

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x5ac80	0x5ae00	False	0.0282652381362	data	2.14570825877	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-23:30:03.114899	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57875	8.8.8.8	192.168.2.3
01/13/22-23:30:09.487899	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54154	8.8.8.8	192.168.2.3
01/13/22-23:30:16.674902	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
01/13/22-23:30:23.300895	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.3
01/13/22-23:30:29.657068	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60784	8.8.8.8	192.168.2.3
01/13/22-23:31:04.814602	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57106	8.8.8.8	192.168.2.3
01/13/22-23:31:29.966209	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64367	8.8.8.8	192.168.2.3
01/13/22-23:31:49.350900	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50585	8.8.8.8	192.168.2.3
01/13/22-23:31:55.654415	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63456	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 23:30:02.870904922 CET	192.168.2.3	8.8.8.8	0x831b	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:09.373775005 CET	192.168.2.3	8.8.8.8	0xeaa2	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 23:30:16.561302900 CET	192.168.2.3	8.8.8.8	0x9112	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:23.187381983 CET	192.168.2.3	8.8.8.8	0xd6c9	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:29.544877052 CET	192.168.2.3	8.8.8.8	0x9289	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:35.862909079 CET	192.168.2.3	8.8.8.8	0x35ae	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:42.131566048 CET	192.168.2.3	8.8.8.8	0x985e	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:48.426723957 CET	192.168.2.3	8.8.8.8	0xf81b	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:54.613883972 CET	192.168.2.3	8.8.8.8	0x5193	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.355778933 CET	192.168.2.3	8.8.8.8	0xc294	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:04.701240063 CET	192.168.2.3	8.8.8.8	0xf140	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:11.947314024 CET	192.168.2.3	8.8.8.8	0xf671	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:16.616014957 CET	192.168.2.3	8.8.8.8	0x5ddc	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:22.897260904 CET	192.168.2.3	8.8.8.8	0x8ef1	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:29.851943970 CET	192.168.2.3	8.8.8.8	0x1c99	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:36.113398075 CET	192.168.2.3	8.8.8.8	0x885e	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:43.051018000 CET	192.168.2.3	8.8.8.8	0xae31	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:49.237736940 CET	192.168.2.3	8.8.8.8	0x2086	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:55.541038036 CET	192.168.2.3	8.8.8.8	0xde21	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 23:30:03.114898920 CET	8.8.8.8	192.168.2.3	0x831b	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:09.487899065 CET	8.8.8.8	192.168.2.3	0xeaa2	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:16.674901962 CET	8.8.8.8	192.168.2.3	0x9112	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:23.300894976 CET	8.8.8.8	192.168.2.3	0xd6c9	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:29.657068014 CET	8.8.8.8	192.168.2.3	0x9289	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:35.880496979 CET	8.8.8.8	192.168.2.3	0x35ae	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:42.150928020 CET	8.8.8.8	192.168.2.3	0x985e	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:48.446316004 CET	8.8.8.8	192.168.2.3	0xf81b	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:54.632702112 CET	8.8.8.8	192.168.2.3	0x5193	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.375061989 CET	8.8.8.8	192.168.2.3	0xc294	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:04.814601898 CET	8.8.8.8	192.168.2.3	0xf140	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:11.966460943 CET	8.8.8.8	192.168.2.3	0xf671	No error (0)	boyhome5100.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 13, 2022 23:31:16.635252953 CET	8.8.8.8	192.168.2.3	0x5ddc	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:22.916559935 CET	8.8.8.8	192.168.2.3	0x8ef1	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:29.966208935 CET	8.8.8.8	192.168.2.3	0x1c99	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:36.133018017 CET	8.8.8.8	192.168.2.3	0x885e	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:43.070338964 CET	8.8.8.8	192.168.2.3	0xae31	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:49.350899935 CET	8.8.8.8	192.168.2.3	0x2086	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:55.654414892 CET	8.8.8.8	192.168.2.3	0xde21	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: filedata.exe PID: 6760 Parent PID: 5712

General

Start time:	23:29:52
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\filedata.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\filedata.exe"
Imagebase:	0x400000
File size:	784599 bytes
MD5 hash:	2CE21C68E4D03F35248689663DC820DE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.300538390.00000000023A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.300538390.00000000023A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.300538390.00000000023A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.300538390.00000000023A0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: filedata.exe PID: 6220 Parent PID: 6760

General

Start time:	23:29:54
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\filedata.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\filedata.exe"
Imagebase:	0x400000
File size:	784599 bytes
MD5 hash:	2CE21C68E4D03F35248689663DC820DE
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: 00000005.00000000.298557071.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.298557071.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.298557071.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.561118810.00000000023B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.561118810.00000000023B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.561118810.00000000023B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.561118810.00000000023B0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563662225.00000000053E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563662225.00000000053E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.561439821.00000000027A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.564073879.0000000005420000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.564073879.0000000005420000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.297190479.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.297190479.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.297190479.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.562912360.0000000004A30000.00000004.00020000.sdmp, Author:

Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.562912360.0000000004A30000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563590904.00000000053D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563590904.00000000053D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563438389.00000000053B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563438389.00000000053B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.561228467.00000000023F2000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.561228467.00000000023F2000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000005.00000002.561228467.00000000023F2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.562570219.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000005.00000002.562570219.0000000003B61000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.556140287.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.556140287.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.556140287.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000005.00000002.556140287.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.564478287.0000000005480000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.564478287.0000000005480000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.564299116.0000000005450000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.564299116.0000000005450000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000005.00000002.561605323.00000000027F4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563389843.0000000005390000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563389843.0000000005390000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.562144773.00000000037D5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000005.00000002.562144773.00000000037D5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563083334.0000000004BC0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563083334.0000000004BC0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.563083334.0000000004BC0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563764546.00000000053F0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563764546.00000000053F0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563059058.0000000004BB0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563059058.0000000004BB0000.00000004.00020000.sdmp, Author: Florian Roth

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000001.299308522.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000001.299308522.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000001.299308522.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.562195683.0000000003832000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.559328771.0000000000614000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.559328771.0000000000614000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.559328771.0000000000614000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.561892124.0000000002958000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563366604.0000000005370000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563366604.0000000005370000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.563890986.0000000005400000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.563890986.0000000005400000.00000004.00020000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.562427187.0000000003A5C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.564263969.0000000005440000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.564263969.0000000005440000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: chmac.exe PID: 2812 Parent PID: 3352

General

Start time:	23:30:03
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\dihsw\chmac.exe"
Imagebase:	0x400000
File size:	784599 bytes
MD5 hash:	2CE21C68E4D03F35248689663DC820DE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.330799074.00000000032C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.330799074.00000000032C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.330799074.00000000032C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.330799074.00000000032C0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: chmac.exe PID: 6352 Parent PID: 2812

General

Start time:	23:30:05
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\dihsw\chmac.exe"
Imagebase:	0x400000
File size:	784599 bytes
MD5 hash:	2CE21C68E4D03F35248689663DC820DE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.327164969.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.327164969.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.327164969.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.345221899.000000000364A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.345221899.000000000364A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.345524498.00000000047C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.345524498.00000000047C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.345524498.00000000047C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.345524498.00000000047C0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000001.328667049.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000001.328667049.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000001.328667049.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.345668628.0000000004812000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.345668628.0000000004812000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.345668628.0000000004812000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.345117243.0000000003611000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.345117243.0000000003611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.345117243.0000000003611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.344185437.0000000000627000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.344185437.0000000000627000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.344185437.0000000000627000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.345062402.000000000261E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.343717430.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.343717430.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.343717430.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.343717430.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.325598662.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.325598662.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.325598662.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: chmac.exe PID: 4476 Parent PID: 3352

General

Start time:	23:30:11
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\dihsw\chmac.exe"
Imagebase:	0x400000
File size:	784599 bytes
MD5 hash:	2CE21C68E4D03F35248689663DC820DE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.345786625.0000000003180000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.345786625.0000000003180000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.345786625.0000000003180000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.345786625.0000000003180000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: chmac.exe PID: 6968 Parent PID: 4476

General

Start time:	23:30:14
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\dihsw\chmac.exe"
Imagebase:	0x400000
File size:	784599 bytes
MD5 hash:	2CE21C68E4D03F35248689663DC820DE
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.361160585.0000000004920000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.361160585.0000000004920000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.361160585.0000000004920000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.361160585.0000000004920000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.361229829.0000000004962000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.361229829.0000000004962000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.361229829.0000000004962000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.360739917.00000000006C4000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.360739917.00000000006C4000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.360739917.00000000006C4000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000001.343397650.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000001.343397650.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000001.343397650.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.360475057.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.360475057.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.360475057.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.360475057.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.342661979.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.342661979.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.342661979.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.361051688.000000000381A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.361051688.000000000381A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.341500174.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.341500174.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.341500174.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.360974701.00000000027EE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.361014751.00000000037E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.361014751.00000000037E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.361014751.00000000037E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis