ID: 552739
Sample Name:
E7C92M5C3X5INV0ICERECEIPTC0PY.exe
Cookbook: default.jbs
Time: 17:28:00
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

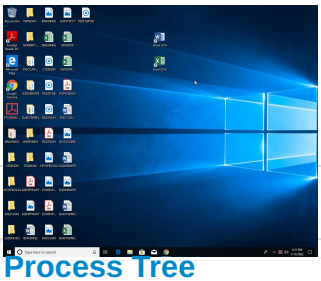
Windows Analysis Report E7C92M5C3X5INV0ICERECEI…

Overview

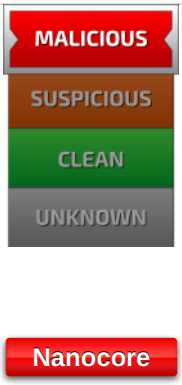
General Information

Sample Name:	E7C92M5C3X5INV0ICERECEIPTC0PY.exe
Analysis ID:	552739
MD5:	b8f28aaee5f699e..
SHA1:	fe881b0a953766d.
SHA256:	b6119b75a4d112..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



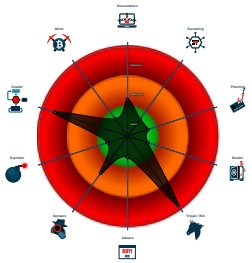
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Detected unpacking (creates a PE fi…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- E7C92M5C3X5INV0ICERECEIPTC0PY.exe (PID: 6192 cmdline: "C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe" MD5: B8F28AAEE5F699EA5CF67E179D7DC459)
  - E7C92M5C3X5INV0ICERECEIPTC0PY.exe (PID: 6348 cmdline: "C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe" MD5: B8F28AAEE5F699EA5CF67E179D7DC459)
- chmac.exe (PID: 6796 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: B8F28AAEE5F699EA5CF67E179D7DC459)
  - chmac.exe (PID: 7144 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: B8F28AAEE5F699EA5CF67E179D7DC459)
- chmac.exe (PID: 2900 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: B8F28AAEE5F699EA5CF67E179D7DC459)
  - chmac.exe (PID: 6188 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: B8F28AAEE5F699EA5CF67E179D7DC459)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "1f8684ca-0835-4252-89d1-4a2b1be1",
  "Group": "boy of john",
  "Domain1": "boyhome5100.duckdns.org",
  "Domain2": "boyhome5100.duckdns.org",
  "Port": 5100,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.329353094.000000000646000.00000004.00000020.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x23625:$x1: NanoCore.ClientPluginHost • 0x23662:$x2: IClientNetworkHost • 0x27195:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000D.00000002.329353094.000000000646000.00000004.00000020.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000002.329353094.000000000646000.00000004.00000020.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xd538:$a: NanoCore • 0x2338d:$a: NanoCore • 0x2339d:$a: NanoCore • 0x235d1:$a: NanoCore • 0x235e5:$a: NanoCore • 0x23625:$a: NanoCore • 0x233ec:$b: ClientPlugin • 0x235ee:$b: ClientPlugin • 0x2362e:$b: ClientPlugin • 0x23513:$c: ProjectData • 0x23f1a:$d: DESCrypto • 0x2b8e6:$e: KeepAlive • 0x298d4:$g: LogClientMessage • 0x25acf:$i: get_Connected • 0x24250:$j: #=q • 0x24280:$j: #=q • 0x2429c:$j: #=q • 0x242cc:$j: #=q • 0x242e8:$j: #=q • 0x24304:$j: #=q • 0x24334:$j: #=q
0000000F.00000002.344015911.00000000023D0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000002.344015911.00000000023D0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 114 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.chmac.exe.47e0000.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
13.2.chmac.exe.47e0000.8.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
13.2.chmac.exe.47e0000.8.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
13.2.chmac.exe.47e0000.8.raw.unpack	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:$j: #=q
15.2.chmac.exe.5ea180.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 403 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:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

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

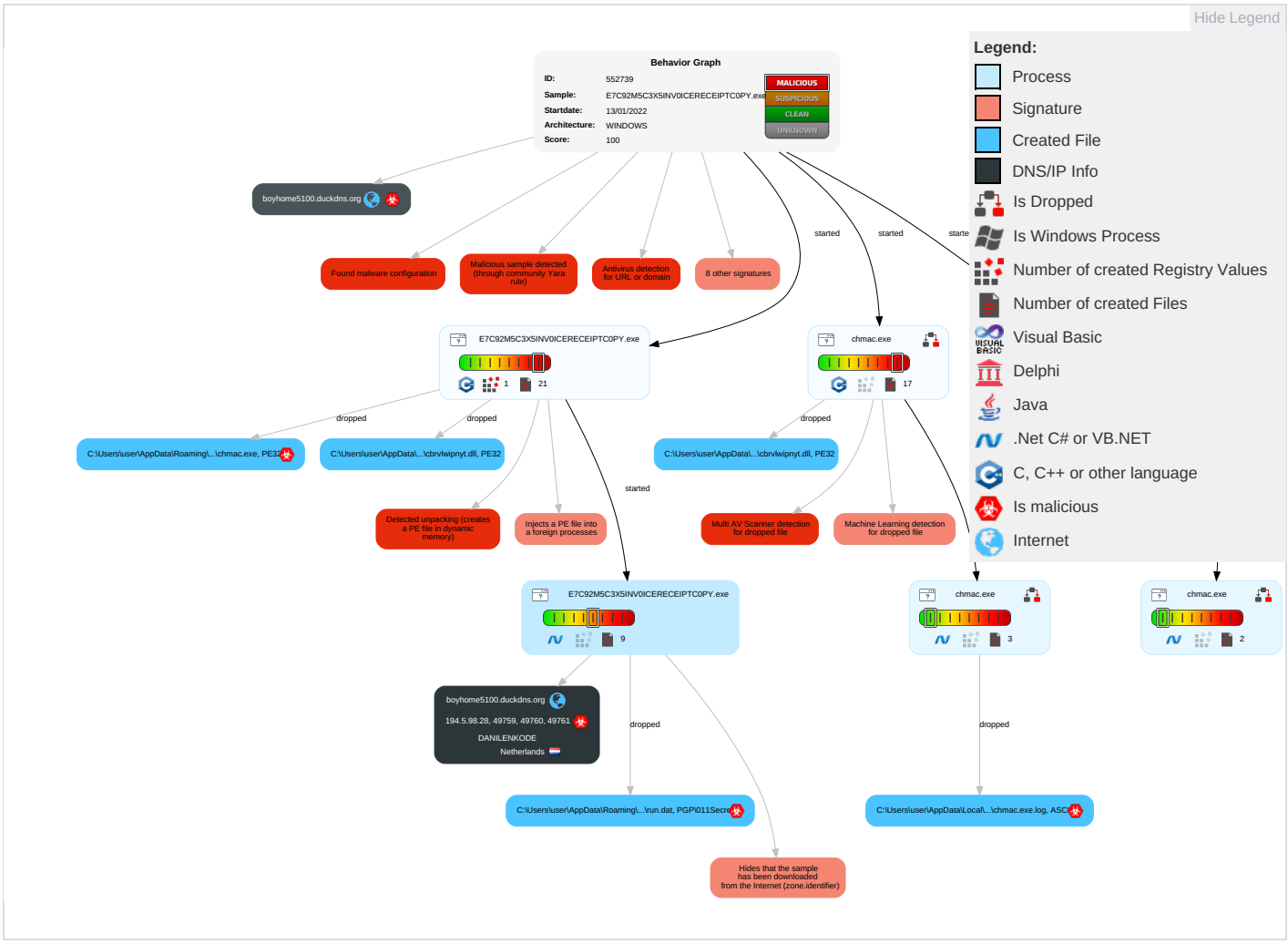
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	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	Encrypted Channel 1	Eavesd Insecur Networ Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco

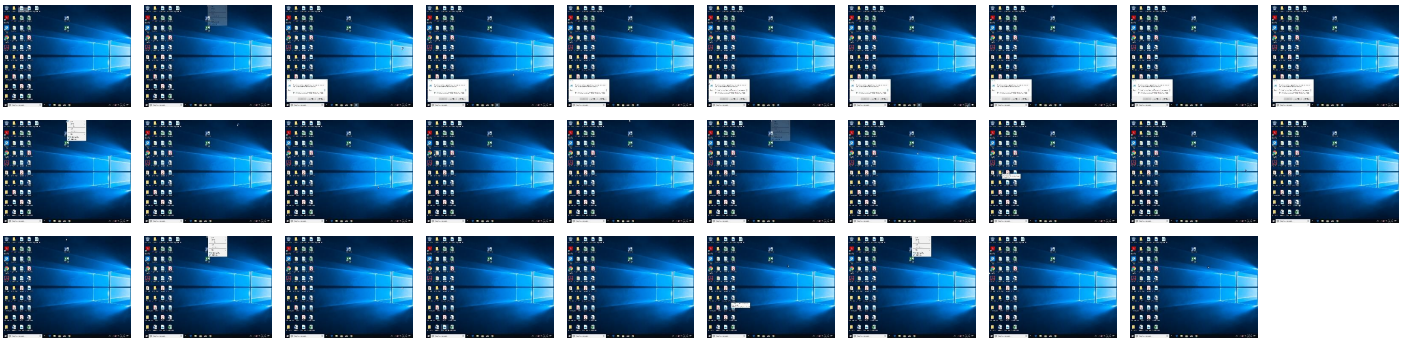
Behavior Graph



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
E7C92M5C3X5INV0ICERECEIPTC0PY.exe	39%	ReversingLabs	Win32.Trojan.Risis	
E7C92M5C3X5INV0ICERECEIPTC0PY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\dihsw\chmac.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dihsw\chmac.exe	39%	ReversingLabs	Win32.Trojan.Risis	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.chmac.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.chmac.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.chmac.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.31f0000.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.chmac.exe.4830000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.1.chmac.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.4970000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.chmac.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.chmac.exe.4970000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.chmac.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.chmac.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.chmac.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.chmac.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.chmac.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.chmac.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.1.chmac.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.chmac.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.1.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.chmac.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.5240000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
3.0.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.E7C92M5C3X5INV0ICERECEIPTC0PY.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
boyhome5100.duckdns.org	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
boyhome5100.duckdns.org	3%	Virustotal		Browse
boyhome5100.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
boyhome5100.duckdns.org	194.5.98.28	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
boyhome5100.duckdns.org	true	• 3%, Virustotal, Browse • Avira URL Cloud: malware	unknown

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	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552739
Start date:	13.01.2022
Start time:	17:28:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	E7C92M5C3X5INV0ICERECEIPTC0PY.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:	28
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@9/12@19/1
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 67.8% (good quality ratio 63%) • Quality average: 78.2% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 85% • 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:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:29:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kyvrnrwl C:\Users\user\AppData\Roaming\dihsw\chmac.exe
17:29:13	API Interceptor	908x Sleep call for process: E7C92M5C3X5INV0ICERECEIPTC0PY.exe modified

Time	Type	Description
17:29:15	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kyvrnrwl C:\Users\user\AppData\Roaming\dihsw\chmac.exe
17:29:18	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:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\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\52wt9dwn8ycpv	
Process:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
File Type:	data
Category:	dropped
Size (bytes):	278527
Entropy (8bit):	7.985804100314347
Encrypted:	false
SSDEEP:	6144:3Z2Zu+K3J3qgR+pad/y3JM8p7+sCbQL1EplfuEEEsruUBNT:0fmtqg8aOJM8p7+n8cl7LsKC
MD5:	592064372FBC1EF3F893085F532C0268
SHA1:	2429979CA086CFD15C5D18535BB44E51B05BD930

C:\Users\user\AppData\Local\Temp\52wt9dwn8ycpv	
SHA-256:	344FB9E236E153E842473ADAE27CBCC1D336F3623B0EC33703AF641A91502299
SHA-512:	C4DDF1293F1B514920F4645BA98C86695B7FC664BAFAEA720E7654BE11CBC0CE18DBD4027E1A0B64432B7A414E5D22421E16FD6F09ECDD27EEC1F3E2C2F670 41
Malicious:	false
Reputation:	low
Preview:	~T.'L&?G.s.? ...j.....Au..$..t..u/0.~..Z.H._.5.c.h......7.f.64lj....3v.\Y.y.w..@..q..j_.y..z.L+oQc.;...\.?.......}..uU.(9........3.p.M.,\.Ku5.x...}ik..........r.zZ.{.....?.&.:..q../P.-.......V.3oQ%... ..sd.M..n..r..a........].*'!~..=T..D..c@m."L.'.&?G..?..c.).\....Au...t.:.u.0.~..Z.H._..c.....2..!'....\..m..j.j.....d...KPb.A...u....y..#..>.Hc.:..'".}..<U.(..o4Q...}.Zh1......w6b.V.\....C.x...g..l... .....y.{...J..h72....I{.r....8...2.., .l.H .[.....lzy..P..dR...D...D..c@m.D..+.&?G..?d.......G...Au..$..t.../0..2{...._...c.F.....!yf...\..'..njqj..,.pp..K?.NA..\.u.......#.....Hc...Q"..KK.X..(...o4.... [fZ.v...v..r.b.V.\..(..E.p..g4..l...>n..w.F...J..h72.....I{.r.....<.2.., .l.H ....lzy..P..dR...D...D..c@m."L.'.&?G.s.?d..........Au..$..t..u/0.~..Z.H._.5.c.h......!'f...\..'..njqj.....dU..KPANA .l..u....y..#.....Hc...Q".}..uU.(..o4Q....fZ.1...v..r.b.V.\....C.x...g..l....>...w.{...J..h72....I{.r.....<.2.., .l.H l

C:\Users\user\AppData\Local\Temp\nsa1F72.tmp\cbrvlwipnyt.dll	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	4608
Entropy (8bit):	3.745710362726581
Encrypted:	false
SSDEEP:	24:e31GSNNH0teIAldax/+Eb2y1gjgFRQ9I6ueeB0Yv8hueeYoNXs+f3SlLRQ0K7ABx:CnUI9voB1GReBvnFbfGFN1RuqSMyO
MD5:	B16AFA20AA77601069F365F82B1D825E
SHA1:	C32C957D00B05E842448F896EF65E5F7F48199D2
SHA-256:	CFAC9E23AAC86191CD988F90E24E97A04F06F2CBF75506EB7B12B20FFEE25AD4
SHA-512:	BF4A01882B8E2E78E1D335A2E61EBF385380E2D3DDAC154FA2CFE8D6046FE5B6593E93A95B418B1E2FEA14A9A1FF0BBEE43D3CBF512DF4898C61953BEBF110 B7
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.......z-...C]..C]..C]Z.M]..C].}B\..C]..B]..C].nG\..C].nC\..C].n.]..C].nA\..C] Rich..C].....PE..L...^+.a.....!..... .....P.....@..... ..H.... .....0.....@..<..... .....text..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsf1F42.tmp	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	data
Category:	dropped
Size (bytes):	316640
Entropy (8bit):	7.77632238767105
Encrypted:	false
SSDEEP:	6144:cVZ2Zu+K3J3qgR+pad/y3JM8p7+sCbQL1EplfuEEEsruUBN:jfmtqg8aOJM8p7+n8cl7LsK
MD5:	B79A0C5F91F041EDFA434C5D619AB8E7
SHA1:	0F0FC02850B3E3615F320C622C7BD45B5ED55E25
SHA-256:	8ED2F8C0AA95FDB5F98D05BDCB6A7DE1FC157C40103F8383E38AFDB09F195BCA
SHA-512:	024944A728DF541FF59C8AE28C6671AE85A81D9134CFCB9E2ADC26A9B85F28FE54C9974F5238CACE5F62947926070768F221F2BDB8868D414A7616A2EAF312D3
Malicious:	false
Reputation:	low
Preview:	.e.....,.....hM.....e.....e.....I..... .....J.....j.....}.....k..... ....

C:\Users\user\AppData\Local\Temp\nsnFE7C.tmp	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	data
Category:	dropped
Size (bytes):	316640
Entropy (8bit):	7.77632238767105
Encrypted:	false
SSDEEP:	6144:cVZ2Zu+K3J3qgR+pad/y3JM8p7+sCbQL1EplfuEEEsruUBN:jfmtqg8aOJM8p7+n8cl7LsK
MD5:	B79A0C5F91F041EDFA434C5D619AB8E7
SHA1:	0F0FC02850B3E3615F320C622C7BD45B5ED55E25
SHA-256:	8ED2F8C0AA95FDB5F98D05BDCB6A7DE1FC157C40103F8383E38AFDB09F195BCA
SHA-512:	024944A728DF541FF59C8AE28C6671AE85A81D9134CFCB9E2ADC26A9B85F28FE54C9974F5238CACE5F62947926070768F221F2BDB8868D414A7616A2EAF312D3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\nsnFE7C.tmp	
Preview:	.e.....,.....hM.....e.....e.....I..... .....J.....j.....}.....k..... ....

C:\Users\user\AppData\Local\Temp\nsnFE7D.tmp\cbrvlwipnyt.dll	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	4608
Entropy (8bit):	3.745710362726581
Encrypted:	false
SSDEEP:	24:e31GSNNH0teIAldax/+Eb2y1gjgFRQ9I6ueeB0Yv8hueeYoNXs+f3SlLRQ0K7ABx:CnUI9voB1GReBvnFbfGFN1RuqSMyO
MD5:	B16AFA20AA77601069F365F82B1D825E
SHA1:	C32C957D00B05E842448F896EF65E5F7F48199D2
SHA-256:	CFAC9E23AAC86191CD988F90E24E97A04F06F2CBF75506EB7B12B20FFEE25AD4
SHA-512:	BF4A01882B8E2E78E1D335A2E61EBF385380E2D3DDAC154FA2CFE8D6046FE5B6593E93A95B418B1E2FEA14A9A1FF0BBEE43D3CBF512DF4898C61953BEBF110B7
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z-...C]..C]..C]Z.M]..C].}B\..C]..B]..C].nG\..C].nC\..C].n.]..C].nA\..C] Rich..C].....PE..L...^+.a.....!..... .....P.....@..... ..H.... .....0.....@..<..... .....text..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsyCEB1.tmp	
Process:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
File Type:	data
Category:	dropped
Size (bytes):	316640
Entropy (8bit):	7.77632238767105
Encrypted:	false
SSDEEP:	6144:cVZ2Zu+K3J3qgR+pad/y3JM8p7+sCbQL1EplfuEEEsruUBN:jfmtqg8aOJM8p7+n8cl7LsK
MD5:	B79A0C5F91F041EDFA434C5D619AB8E7
SHA1:	0F0FC02850B3E3615F320C622C7BD45B5ED55E25
SHA-256:	8ED2F8C0AA95FDB5F98D05BDCB6A7DE1FC157C40103F8383E38AFDB09F195BCA
SHA-512:	024944A728DF541FF59C8AE28C6671AE85A81D9134CFCB9E2ADC26A9B85F28FE54C9974F5238CACE5F62947926070768F221F2BDB8868D414A7616A2EAF312D3
Malicious:	false
Reputation:	low
Preview:	.e.....,.....hM.....e.....e.....I..... .....J.....j.....}.....k..... ....

C:\Users\user\AppData\Local\Temp\nsyCEB2.tmp\cbrvlwipnyt.dll	
Process:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.745710362726581
Encrypted:	false
SSDEEP:	24:e31GSNNH0teIAldax/+Eb2y1gjgFRQ9I6ueeB0Yv8hueeYoNXs+f3SlLRQ0K7ABx:CnUI9voB1GReBvnFbfGFN1RuqSMyO
MD5:	B16AFA20AA77601069F365F82B1D825E
SHA1:	C32C957D00B05E842448F896EF65E5F7F48199D2
SHA-256:	CFAC9E23AAC86191CD988F90E24E97A04F06F2CBF75506EB7B12B20FFEE25AD4
SHA-512:	BF4A01882B8E2E78E1D335A2E61EBF385380E2D3DDAC154FA2CFE8D6046FE5B6593E93A95B418B1E2FEA14A9A1FF0BBEE43D3CBF512DF4898C61953BEBF110B7
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z-...C]..C]..C]Z.M]..C].}B\..C]..B]..C].nG\..C].nC\..C].n.]..C].nA\..C] Rich..C].....PE..L...^+.a.....!..... .....P.....@..... ..H.... .....0.....@..<..... .....text..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\rndtb	
Process:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
File Type:	data
Category:	dropped
Size (bytes):	7379
Entropy (8bit):	6.086446093141458
Encrypted:	false
SSDEEP:	96:aQrklevJa2GjLXU4ky2VxQTvgSmM/1/CXsqpU/1UCHndPXwm8x5v58fVhfuvTavD:acEexmjLXUHlPKGEXmh8bu7iw9XS/
MD5:	8AE020DB6D40782CC969512C8F587F18
SHA1:	163D8340E03E30E75987A8EB55953E607DDBB6DD
SHA-256:	50DB2FAFE64D4FEB4F8CFE4BC68F01C3D62BAA33214EDAE64CBC87C4F26CB86E
SHA-512:	6E1C4FED647BF32FB4AF7B84CDAEEC97771F7B7ABE5312BEF0A275E237C03F72E202AD4930D38B9A8B1C63E7BF44F9C120237C884E725EA8E602A2B07A2386F A
Malicious:	false
Reputation:	low
Preview:	..0))~....i|.....)8..8<n.8..8<n...!).n%Q)))...)(.5(.9.n!y.&))).n..~.(.5(.9.n!y..))).n..~.(.5(.9.n!y..))).n.~.(.5(.9.n!y..))).n.~.9-.c.1...,,n5.n..~..n9..-\.n..v..n..v%.-.\..9. ..n.,~%.-.n%.....\.))))..-M..T.%(...(...(..j.(..j.(...(.....9.q.5 .q.u.l..*..(..j..n18..n.,.%.)))).mM-L))).-M6.....n.....5)~..zz8..8<n!.n1.)dn5.I.n1.).v9.=.~!.m.-.n%.n1.)i.v1.*.n!.~%....5).?#...+))..+)).=)..(....+)) ..+)).1).6...}+)).s+)).1)~....Q8..8<n..n!9))).n..n%..!).?.n%.)).n%i.n%.n!q.n!...=.))..o.n1.1...).m6..}6..n..1...).m6..}6..+.1...).m..y..(....*))y..&((.n..8.n.y(.1.s(((.n....)./...).0.n.*))).n.....-)~....i8..8<n..n!Q))).n.n%..!).?.n%.)).n%i.n%.n!q.n!....-))..8..))).n1.1...).m6.}6.n5.1...).m6.}6.n9.1....m6.}6.n=\.1...,.m>.u>.n..1...+.m6.}6...1...).m..y.?#...)))y..%((.n...A).1.n.. vA.*.@(.A(.=(.9(.5(.1.``((.n....)./...).0.n.*))).n.....=)~....E.n!9))).n..n%..!).?.n%.)).n%i.n%.n!q.n!....,))..o.n1.1...).m6..}6..n5.1...).m6..}6..+.1...).m..y.6...P)))y.M%((.n..7(.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.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
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\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Od4:J
MD5:	170DE553555F47CB1040AB5CB7E8A9C7
SHA1:	497E879B24B89AD70EB5540642A15C684A52ABB1
SHA-256:	ECD813474B34BF576F7746E686B1D5A90986D7C87D4D117C545DC000FA19E09B
SHA-512:	2C5F531E7DB29C6C9171FAD7B9C9FE8A5F41BD29B06BDB2490F03B45D9E8C5B964F7938C763B2FD110D2A4FD3B254F2736677AA81C1AFB71B276E675BA1D66 B
Malicious:	**true**
Preview:	..LE...H

C:\Users\user\AppData\Roaming\dihsw\chmac.exe	
Process:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	modified
Size (bytes):	396620
Entropy (8bit):	7.179508254773959
Encrypted:	false
SSDEEP:	6144:FwaLxL89xigqENN3jDaKztZW/oMap1UQx194XGDQEPQ:Bo94gBHvz/UoMap1UIAEPQ
MD5:	B8F28AAEE5F699EA5CF67E179D7DC459
SHA1:	FE881B0A953766DA485D24FBBDB0AED377D92446
SHA-256:	B6119B75A4D112FEF0D8AA1A5B8BAA9F3A2A5A9385BD3C669B4D628FCB3318CC

C:\Users\user\AppData\Roaming\dihsw\chmac.exe	
SHA-512:	0992F2C31FA187C38C0DC05DA1FCB04CD52A254B27C3F35AD30D0DBB68FC2E916896490ADC24867FDB2047A9A46019BEC8C5868452755FB17B0F2A423C90CB4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....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):	7.179508254773959
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:	E7C92M5C3X5INV0ICERECEIPTC0PY.exe
File size:	396620
MD5:	b8f28aaee5f699ea5cf67e179d7dc459
SHA1:	fe881b0a953766da485d24fbbdb0aed377d92446
SHA256:	b6119b75a4d112fef0d8aa1a5b8baa9f3a2a5a9385bd3c669b4d628fcb3318cc
SHA512:	0992f2c31fa187c38c0dc05da1fcb04cd52a254b27c3f35ad30d0dbb68fc2e916896490adc24867fdb2047a9a46019bec8c5868452755fb17b0f2a423c90cbf4
SSDEEP:	6144:FwaLxL89xigqENN3jDaKztZW/oMap1UQx194XGDQEPQ:Bo94gBHvz/UoMap1UIAEPQ
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:	13331333690d37c8

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

General

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
.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	0x19d20	0x19e00	False	0.106931234903	data	3.00487775819	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
01/13/22-17:29:15.113964	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59762	8.8.8.8	192.168.2.7
01/13/22-17:29:21.979236	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54329	8.8.8.8	192.168.2.7
01/13/22-17:29:36.637938	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59451	8.8.8.8	192.168.2.7
01/13/22-17:29:50.178656	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54230	8.8.8.8	192.168.2.7
01/13/22-17:30:03.223529	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50452	8.8.8.8	192.168.2.7
01/13/22-17:30:09.748812	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59310	8.8.8.8	192.168.2.7
01/13/22-17:30:22.682064	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56680	8.8.8.8	192.168.2.7
01/13/22-17:30:42.134881	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50290	8.8.8.8	192.168.2.7
01/13/22-17:31:13.772186	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59179	8.8.8.8	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 17:29:14.999522924 CET	192.168.2.7	8.8.8.8	0xccd1	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:21.861089945 CET	192.168.2.7	8.8.8.8	0xf581	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:30.258733034 CET	192.168.2.7	8.8.8.8	0x6443	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:36.526283979 CET	192.168.2.7	8.8.8.8	0x871f	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:43.826831102 CET	192.168.2.7	8.8.8.8	0xdd02	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:50.066612005 CET	192.168.2.7	8.8.8.8	0x6e23	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:56.416671991 CET	192.168.2.7	8.8.8.8	0x6042	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:03.054822922 CET	192.168.2.7	8.8.8.8	0x64cb	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:09.633110046 CET	192.168.2.7	8.8.8.8	0x908b	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:16.111844063 CET	192.168.2.7	8.8.8.8	0x3e04	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:22.568350077 CET	192.168.2.7	8.8.8.8	0x9aea	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:29.601330042 CET	192.168.2.7	8.8.8.8	0xf919	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:35.808698893 CET	192.168.2.7	8.8.8.8	0x4476	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:42.022706032 CET	192.168.2.7	8.8.8.8	0x2bda	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:48.632338047 CET	192.168.2.7	8.8.8.8	0xf688	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:54.873039007 CET	192.168.2.7	8.8.8.8	0x4574	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:31:00.079221964 CET	192.168.2.7	8.8.8.8	0xc9c1	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:31:07.614753008 CET	192.168.2.7	8.8.8.8	0xf466	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 17:31:13.658898115 CET	192.168.2.7	8.8.8.8	0x3c78	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

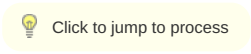
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 17:29:15.113964081 CET	8.8.8.8	192.168.2.7	0xccd1	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:21.979235888 CET	8.8.8.8	192.168.2.7	0xf581	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:30.278124094 CET	8.8.8.8	192.168.2.7	0x6443	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:36.637938023 CET	8.8.8.8	192.168.2.7	0x871f	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:43.852618933 CET	8.8.8.8	192.168.2.7	0xdd02	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:50.178656101 CET	8.8.8.8	192.168.2.7	0x6e23	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:29:56.438747883 CET	8.8.8.8	192.168.2.7	0x6042	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:03.223529100 CET	8.8.8.8	192.168.2.7	0x64cb	No error (0)	boyhome510 0.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 17:30:09.748811960 CET	8.8.8.8	192.168.2.7	0x908b	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:16.131125927 CET	8.8.8.8	192.168.2.7	0x3e04	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:22.682064056 CET	8.8.8.8	192.168.2.7	0x9aea	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:29.618391991 CET	8.8.8.8	192.168.2.7	0xf919	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:35.828156948 CET	8.8.8.8	192.168.2.7	0x4476	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:42.134881020 CET	8.8.8.8	192.168.2.7	0x2bda	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:48.651621103 CET	8.8.8.8	192.168.2.7	0xf688	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:30:54.893079042 CET	8.8.8.8	192.168.2.7	0x4574	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:31:00.098967075 CET	8.8.8.8	192.168.2.7	0xc9c1	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:31:07.634083986 CET	8.8.8.8	192.168.2.7	0xf466	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 17:31:13.772186041 CET	8.8.8.8	192.168.2.7	0x3c78	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: E7C92M5C3X5INV0ICERECEIPTC0PY.exe PID: 6192 Parent PID: 1148

General

Start time:	17:29:04
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe"
Imagebase:	0x400000
File size:	396620 bytes
MD5 hash:	B8F28AAEE5F699EA5CF67E179D7DC459
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: 00000001.00000002.279840605.00000000031A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.279840605.00000000031A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.279840605.00000000031A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.279840605.00000000031A0000.00000004.00000001.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: E7C92M5C3X5INV0ICERECEIPTC0PY.exe PID: 6348 Parent PID: 6192

General

Start time:	17:29:06
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\E7C92M5C3X5INV0ICERECEIPTC0PY.exe"
Imagebase:	0x400000
File size:	396620 bytes
MD5 hash:	B8F28AAEE5F699EA5CF67E179D7DC459
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: 00000003.00000001.277777904.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000001.277777904.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000001.277777904.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000001.277777904.0000000000400000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.537875964.0000000004FB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.537875964.0000000004FB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.276176982.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.276176982.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.276176982.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.537160483.0000000004972000.00000040.00000001.sdmp, Author:

	Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.537160483.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.537160483.0000000004972000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.535932068.0000000002741000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.532960247.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.532960247.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.532960247.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.532960247.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.536653238.00000000037D2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.538012493.0000000005240000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.538012493.0000000005240000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.538012493.0000000005240000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.537074209.0000000004920000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.537074209.0000000004920000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.537074209.0000000004920000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.537074209.0000000004920000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.277052360.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.277052360.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.277052360.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.533535675.0000000000605000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.533535675.0000000000605000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.533535675.0000000000605000.00000004.00000020.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: 6796 Parent PID: 3292

General

Start time:	17:29:15
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:	396620 bytes
MD5 hash:	B8F28AAEE5F699EA5CF67E179D7DC459
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: 0000000A.00000002.315161594.00000000022E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.315161594.00000000022E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.315161594.00000000022E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.315161594.00000000022E0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: chmac.exe PID: 7144 Parent PID: 6796

General

Start time:	17:29:18
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:	396620 bytes
MD5 hash:	B8F28AAEE5F699EA5CF67E179D7DC459
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: 0000000D.00000002.329353094.0000000000646000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.329353094.0000000000646000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.329353094.0000000000646000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.329778685.000000000264E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.330027295.00000000047E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.330027295.00000000047E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.330027295.00000000047E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.330027295.00000000047E0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.330114901.0000000004832000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.330114901.0000000004832000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.330114901.0000000004832000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.310714262.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.310714262.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.310714262.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.329125681.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.329125681.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.329125681.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.329125681.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.329836046.0000000003641000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.329836046.0000000003641000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.329836046.0000000003641000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.311827884.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.311827884.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.311827884.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000001.313770217.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000001.313770217.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000001.313770217.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.329889778.000000000367A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.329889778.000000000367A000.00000004.00000001.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: 2900 Parent PID: 3292

General

Start time:	17:29:23
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:	396620 bytes
MD5 hash:	B8F28AAEE5F699EA5CF67E179D7DC459
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: 0000000E.00000002.326347561.0000000003050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.326347561.0000000003050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.326347561.0000000003050000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.326347561.0000000003050000.00000004.00000001.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: 6188 Parent PID: 2900

General

Start time:	17:29:26
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:	396620 bytes
MD5 hash:	B8F28AAEE5F699EA5CF67E179D7DC459
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: 0000000F.00000002.344015911.00000000023D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.344015911.00000000023D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.344015911.00000000023D0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.344015911.00000000023D0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.344478918.0000000003871000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.344478918.0000000003871000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.344478918.0000000003871000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.344439320.000000000287E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.322006756.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.322006756.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.322006756.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.323952546.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.323952546.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.323952546.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000001.324557276.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000001.324557276.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000001.324557276.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.344643169.0000000004972000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.344643169.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.344643169.0000000004972000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.341426483.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.341426483.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.341426483.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.341426483.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.341593933.00000000005D5000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.341593933.00000000005D5000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.341593933.00000000005D5000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.344514472.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.344514472.00000000038AA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis