ID: 552628
Sample Name:
G2M8C76V_INV0ICE_RECEIPT.exe
Cookbook: default.jbs
Time: 15:31:20
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

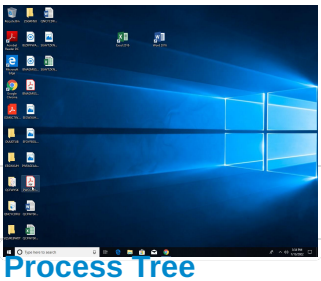
Windows Analysis Report G2M8C76V_INV0ICE_RECEIP…

Overview

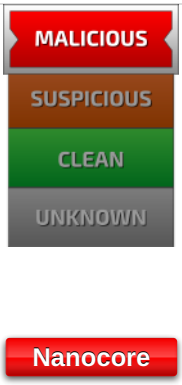
General Information

Sample Name:	G2M8C76V_INV0ICE_RECEIPT.exe
Analysis ID:	552628
MD5:	d272e884f59ff9d…
SHA1:	b9013dcffc28e17..
SHA256:	94a00e5d13eebc..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



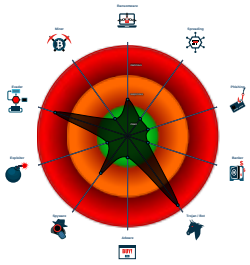
Nanocore

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

Signatures

- Found malware configuration
- 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…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- G2M8C76V_INV0ICE_RECEIPT.exe (PID: 6964 cmdline: "C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe" MD5: D272E884F59FF9D7921619F88766709D)
  - G2M8C76V_INV0ICE_RECEIPT.exe (PID: 7092 cmdline: "C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe" MD5: D272E884F59FF9D7921619F88766709D)
- chmac.exe (PID: 6288 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: D272E884F59FF9D7921619F88766709D)
  - chmac.exe (PID: 6556 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: D272E884F59FF9D7921619F88766709D)
- chmac.exe (PID: 6760 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: D272E884F59FF9D7921619F88766709D)
  - chmac.exe (PID: 6820 cmdline: "C:\Users\user\AppData\Roaming\dihsw\chmac.exe" MD5: D272E884F59FF9D7921619F88766709D)
- **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
0000000E.00000002.341257135.000000000373 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x123e5:$x1: NanoCore.ClientPluginHost • 0x12422:$x2: IClientNetworkHost • 0x15f55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.341257135.000000000373 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000002.341257135.000000000373 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1214d:$a: NanoCore • 0x1215d:$a: NanoCore • 0x12391:$a: NanoCore • 0x123a5:$a: NanoCore • 0x123e5:$a: NanoCore • 0x121ac:$b: ClientPlugin • 0x123ae:$b: ClientPlugin • 0x123ee:$b: ClientPlugin • 0x122d3:$c: ProjectData • 0x12cda:$d: DESCrypto • 0x1a6a6:$e: KeepAlive • 0x18694:$g: LogClientMessage • 0x1488f:$i: get_Connected • 0x13010:$j: #=q • 0x13040:$j: #=q • 0x1305c:$j: #=q • 0x1308c:$j: #=q • 0x130a8:$j: #=q • 0x130c4:$j: #=q • 0x130f4:$j: #=q • 0x13110:$j: #=q
0000000E.00000000.322700795.000000000041 4000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x111e5:$x1: NanoCore.ClientPluginHost • 0x11222:$x2: IClientNetworkHost • 0x14d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000000.322700795.000000000041 4000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 92 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.chmac.exe.2906888.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
16.2.chmac.exe.2906888.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
14.2.chmac.exe.400000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
14.2.chmac.exe.400000.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2135d:$x1: NanoCore Client.exe • 0x215e5:$x2: NanoCore.ClientPluginHost • 0x22c1e:$s1: PluginCommand • 0x22c12:$s2: FileCommand • 0x23ac3:$s3: PipeExists • 0x2987a:$s4: PipeCreated • 0x2160f:$s5: IClientLoggingHost
14.2.chmac.exe.400000.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 341 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

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

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

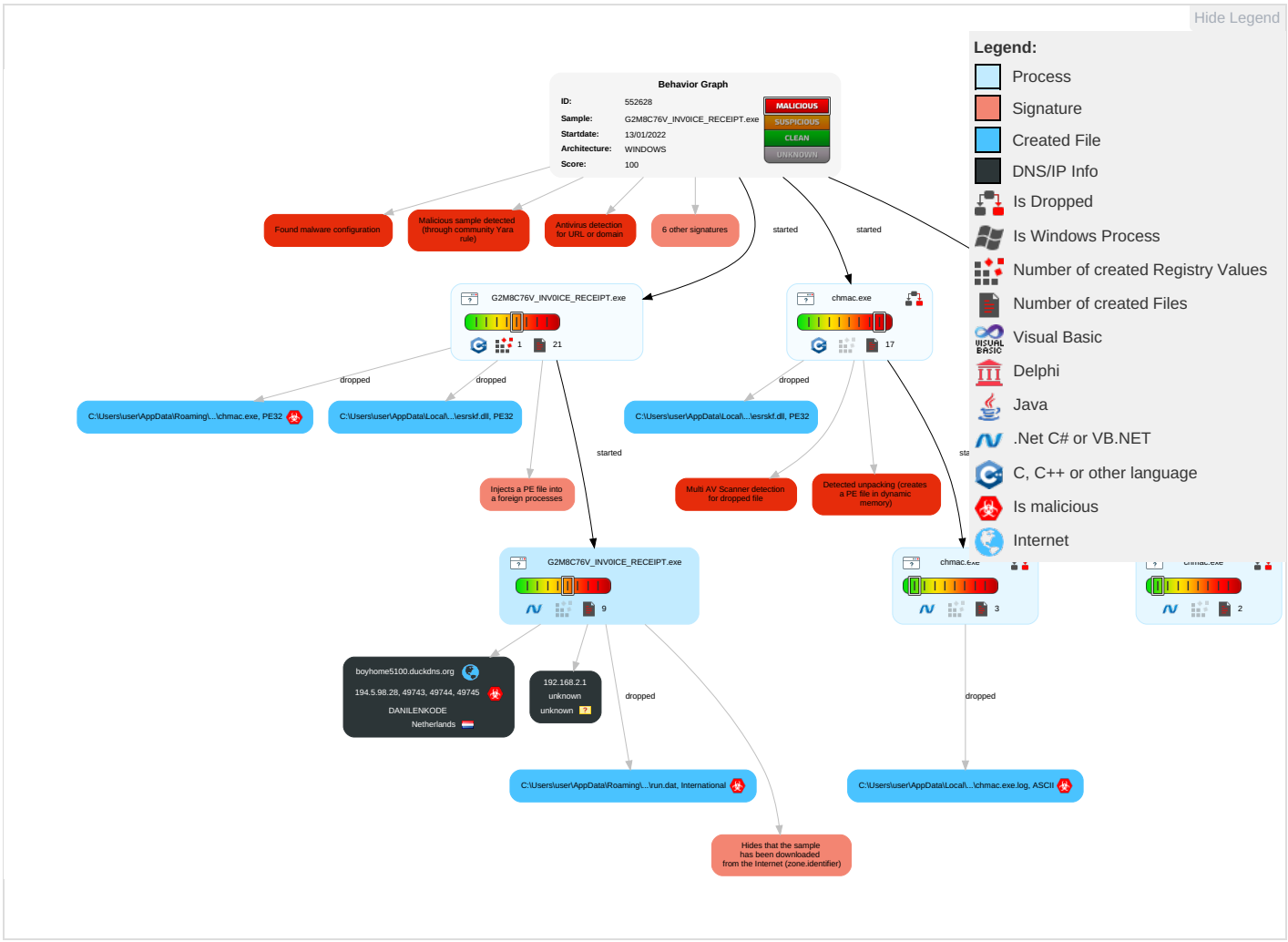
Yara detected Nanocore RAT

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 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	Encrypted Channel 1	Eavesd Insecur Networ Commu
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	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 1	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 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
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

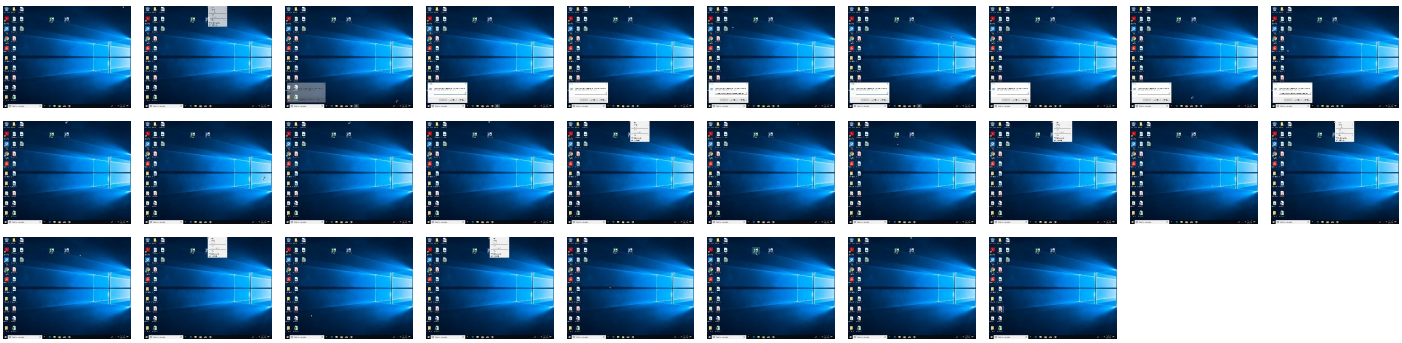
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\dihsw\chmac.exe	42%	ReversingLabs	Win32.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.0.chmac.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.chmac.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.chmac.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.chmac.exe.4830000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.chmac.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.G2M8C76V_INV0ICE_RECEIPT.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.G2M8C76V_INV0ICE_RECEIPT.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.G2M8C76V_INV0ICE_RECEIPT.exe.30f0000.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.1.chmac.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.G2M8C76V_INV0ICE_RECEIPT.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
14.0.chmac.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.G2M8C76V_INV0ICE_RECEIPT.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.G2M8C76V_INV0ICE_RECEIPT.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.chmac.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.1.G2M8C76V_INV0ICE_RECEIPT.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.chmac.exe.2500000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.G2M8C76V_INV0ICE_RECEIPT.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.chmac.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.1.chmac.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.chmac.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.G2M8C76V_INV0ICE_RECEIPT.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.chmac.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.chmac.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.chmac.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.chmac.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.chmac.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
boyhome5100.duckdns.org	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
boyhome5100.duckdns.org	2%	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	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
boyhome5100.duckdns.org	true	• 2%, 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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552628
Start date:	13.01.2022
Start time:	15:31:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	G2M8C76V_INV0ICE_RECEIPT.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:	29
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@19/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 70.6% (good quality ratio 65.6%) • Quality average: 78.3% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 88% • 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
15:32:17	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kyvrnrwl C:\Users\user\AppData\Roaming\dihsw\chmac.exe
15:32:22	API Interceptor	959x Sleep call for process: G2M8C76V_INV0ICE_RECEIPT.exe modified
15:32:25	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kyvrnrwl C:\Users\user\AppData\Roaming\dihsw\chmac.exe
15:32:27	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\56mc2ilzkdt85ppfm	
Process:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe
File Type:	data
Category:	dropped
Size (bytes):	278527
Entropy (8bit):	7.984440804169609
Encrypted:	false
SSDEEP:	6144:ANMYeemSX268bMvy0lOGYLjTDNe4bKtB5u85S1wJLYoAlwYJuDNW:AqYeyX6Yq0lPYXNdb0Hw1wJLYoAlLgW
MD5:	E2674E39313EB905BEDB38EE4A90EB82
SHA1:	7EC20D0AD4E70C7621B7D0D836CA7C22029B8A9E
SHA-256:	91CBC859051888ECD50E3765A1A0AE9280DBD540A32A272D6D153F969CEA606D
SHA-512:	FA36A87ED16623BC62B76663F2DFAB3097DA69107CB091BD3BD4C677415F09E5CAF329F06FB566CF8A29CBDE7E50CCACDDFBE44BC125532BF0D9F6AF9D0B0 52B
Malicious:	false
Reputation:	low
Preview:	...np.y6k.x..@.....M...v...,M.6.'..X..._...1v.,l....8.Z6..H.2B.?.K..<.Lp.,h.].PYEG.t.BlU...Z.7.F....%.#..z..Z.3.....`P...?.R).....0.....$\|.tW`../.ugo..<.c]}D.nT)...0&.i.....v. {...g...S.X2;v....r`.7...P-.3Rq8.....S..?. ..p.y...x.vc.....\|.M.}..o,..,M.6.'L.X..._[..1v.,l.\.. .VZ.{\|....t...B.?.H.....M.&M_F..l^Q.{..#....k.r0...G!...Ba.3.....6.D=...B.lX...8.Ob.A... q=....Cw....Z...."fR"..l..V...@....*;qe.P2..`...B.!..s..L..Q?`..R...Ki.SH..=D$..r....2a}M...X.....S..v...p.yg,.x?.@.....|.M...v...,..6....;..._t..1vs,l.... I.Z..{|.o..P....?Fa9wj.M....F...^Ql{...a...X.r....GG..TBD...k(...P.D=...bR.X..L8.....q=..<.C...P.]...CA?R"U.l..d.....*;qe.P2..b..dB.!..s.....?`..R...Ki.SB....$..r....2a}M...X.....S..?. ..p.y.k.x?2@.....\|.M...v...,M.6.'.. X..._...1v.,l.... ..Z..{\|.o..P...B.?...U...M.&..F.zl^Q.{..#....X.r....GG..TBa.3.....6.D=...bb.X...8.....q=....Cw....Z...."fR"..l.j...@....*;qe.P2..`...B.!..s.....?`..R...Ki.SB....$.

C:\Users\user\AppData\Local\Temp\nfjvhlc	
Process:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe
File Type:	data
Category:	dropped
Size (bytes):	7448
Entropy (8bit):	6.084978183064926
Encrypted:	false
SSDEEP:	192:efAApVIRgy4M0Ag13vj/O7s7Pb/T8MEAGLVrW1nU8sj:kqb0bF/NPbAMKLVrMnUv
MD5:	812162B475D941A12A193D8C085597E6

C:\Users\user\AppData\Local\Temp\nfjvhlc	
SHA1:	9B4B7CD34860F8FA19B0B5154DBB7F69CFC99489
SHA-256:	C89928AC7C6B93AB283B1197CA645AF22DC77FBFA5E066EDEEAE3402A952ED47
SHA-512:	BFAB4487C5434108FC063A6FCE997543B720F179674C32366910A25DB366FC41179A5492719288C2ABBB2677C510FFD41EDE53B98ED2F44155B8DA50FBE33722
Malicious:	false
Reputation:	low
Preview:	;....i.....T....4.T....<....]..... .....g...<.....,..8.....g...<<.....$..0.....g...<1.....\..(.....g...<V.....T..`.. .....T!!..k..4..@i..< .[..<...i.<i..g S.2....i.<!..g b.....@...<..... ..)....,...$...\...T.. .4...<.....i.....,i.....!..<....].. ....)i....i.....i?.b...i....T.....i..i.....i..i.i.i.i.S...i.S ...i..i..i.i....i..i..i?.b.....^.<."..<."..b.....5.<."..<."..b....y.<."..<."..b...i.....T....<]......g.,.....i..^..i.....i.. ....@<.....T..i..k....[....,...8g.<k...S3....,...8."....T.g..,....5.<#....<&.....g.<....<.....]......i..i?.b ..i.....T....<]......g.T.....i..^..i.....i.....@<. ...T.j...i..k....[....T...`i..k...S3....T...`i.. k...#3...T...`i...[....2!...T...`g.<k...S3"...T...`.....T.g..T....^.<>....<A.....i.<i.....<.....]......i..i?.b...i....]......g.@.....i..^..i.....i.....@<.!...T..i..k....[....@...<i..k...S3 ....@...<."....T.g..@...y.<.....<.....

C:\Users\user\AppData\Local\Temp\nsiCC1.tmp	
Process:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe
File Type:	data
Category:	dropped
Size (bytes):	317856
Entropy (8bit):	7.76643048605343
Encrypted:	false
SSDEEP:	6144:2jCLNMYeemSX268bMvy0lOGYLjTDNe4bKtB5u85S1wJLYoAlwYJuDN:2eqYeyX6Yq0lPYXNdb0Hw1wJLYoAlLg
MD5:	C2D44B063B4B0AABF482FFB2E1074145
SHA1:	F5EFA683BD7E7FCDF848C26F8E8A81D9DDA9CFE6
SHA-256:	0994AF1254D390C551AD60759AF35F2267CB7324182C2087772D51D89DB9C004
SHA-512:	BB831F963B4213E5B23403141261BE8C8C68EBEFE087EE66B4C5783A343FE93DB8A081CCC7AEF6998861371D51FFE4B9FFEB39A3AAC53FAC8C5C9D14F94FC795
Malicious:	false
Reputation:	low
Preview:	yj.....,.....a....P.....i.....aj..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsiCC2.tmp\esrskf.dll	
Process:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7711135978980614
Encrypted:	false
SSDEEP:	24:e31GSNNN0teIAJdax/+YZVy0NVxagHCueecv8hueeYoNXs+f3SlLRQ0K7ABPnRug:CnaI9ro3ngnFbfGFN1RuqSR
MD5:	CA6B2E72403972AE585025A81040FC44
SHA1:	BDA160D06EE5611B6CFE53F048CC00526941A1D4
SHA-256:	E0932A5438FFEE964EF9DEB10C5C5F187B12B319894552BA062A36E93EABBBF8
SHA-512:	48283C382D8C95DC96E193EAE541F6E86FFA43D107D0F739F1FFEA779364EFC0562A094C167F65ADCFD97B37BA6A31F561E237E92601F908AD7AAC87FF56B2ED
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....0.a.....!..... ....P.....@..... ..H... .....0.....@..<..... .....text...B..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsq5FC3.tmp	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	data
Category:	dropped
Size (bytes):	317856
Entropy (8bit):	7.76643048605343
Encrypted:	false
SSDEEP:	6144:2jCLNMYeemSX268bMvy0lOGYLjTDNe4bKtB5u85S1wJLYoAlwYJuDN:2eqYeyX6Yq0lPYXNdb0Hw1wJLYoAlLg
MD5:	C2D44B063B4B0AABF482FFB2E1074145
SHA1:	F5EFA683BD7E7FCDF848C26F8E8A81D9DDA9CFE6
SHA-256:	0994AF1254D390C551AD60759AF35F2267CB7324182C2087772D51D89DB9C004
SHA-512:	BB831F963B4213E5B23403141261BE8C8C68EBEFE087EE66B4C5783A343FE93DB8A081CCC7AEF6998861371D51FFE4B9FFEB39A3AAC53FAC8C5C9D14F94FC795
Malicious:	false

C:\Users\user\AppData\Local\Temp\nsq5FC3.tmp	
Reputation:	low
Preview:	yj.....,.....a....P.....i.....aj..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsq5FC4.tmp\esrskf.dll	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7711135978980614
Encrypted:	false
SSDEEP:	24:e31GSNNN0teIAJdax/+YZVy0NVxagHCueecv8hueeYoNXs+f3SlLRQ0K7ABPnRug:CnaI9ro3ngnFbfGFN1RuqSR
MD5:	CA6B2E72403972AE585025A81040FC44
SHA1:	BDA160D06EE5611B6CFE53F048CC00526941A1D4
SHA-256:	E0932A5438FFEE964EF9DEB10C5C5F187B12B319894552BA062A36E93EABBBF8
SHA-512:	48283C382D8C95DC96E193EAE541F6E86FFA43D107D0F739F1FFEA779364EFC0562A094C167F65ADCFD97B37BA6A31F561E237E92601F908AD7AAC87FF56B2E D
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....0.a.....!..... .....P.....@..... ..H... .....0.....@..<..... .....text...B..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsx3DC4.tmp	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	data
Category:	dropped
Size (bytes):	317856
Entropy (8bit):	7.76643048605343
Encrypted:	false
SSDEEP:	6144:2jCLNMYeemSX268bMvy0lOGYLjTDNe4bKtB5u85S1wJLYoAlwYJuDN:2eqYeyX6Yq0lPYXNdb0Hw1wJLYoAlLg
MD5:	C2D44B063B4B0AABF482FFB2E1074145
SHA1:	F5EFA683BD7E7FCDF848C26F8E8A81D9DDA9CFE6
SHA-256:	0994AF1254D390C551AD60759AF35F2267CB7324182C2087772D51D89DB9C004
SHA-512:	BB831F963B4213E5B23403141261BE8C8C68EBEFE087EE66B4C5783A343FE93DB8A081CCC7AEF6998861371D51FFE4B9FFEB39A3AAC53FAC8C5C9D14F94FC7 95
Malicious:	false
Reputation:	low
Preview:	yj.....,.....a....P.....i.....aj..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsx3DC5.tmp\esrskf.dll	
Process:	C:\Users\user\AppData\Roaming\dihsw\chmac.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7711135978980614
Encrypted:	false
SSDEEP:	24:e31GSNNN0teIAJdax/+YZVy0NVxagHCueecv8hueeYoNXs+f3SlLRQ0K7ABPnRug:CnaI9ro3ngnFbfGFN1RuqSR
MD5:	CA6B2E72403972AE585025A81040FC44
SHA1:	BDA160D06EE5611B6CFE53F048CC00526941A1D4
SHA-256:	E0932A5438FFEE964EF9DEB10C5C5F187B12B319894552BA062A36E93EABBBF8
SHA-512:	48283C382D8C95DC96E193EAE541F6E86FFA43D107D0F739F1FFEA779364EFC0562A094C167F65ADCFD97B37BA6A31F561E237E92601F908AD7AAC87FF56B2E D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\nsx3DC5.tmp\esrskf.dll	
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....0.a.....!..... .....P.....@..... ..H... .....0.....@..<.....text...B..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.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
Reputation:	moderate, very likely benign file
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\G2M8C76V_INV0ICE_RECEIPT.exe
File Type:	International EBCDIC text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:JX98:o
MD5:	96A85767F76F3E5FC753A622A56C5315
SHA1:	67832A8FDABC53BB4AF9DFEB37705D62A32559A5
SHA-256:	8AE24E6F0625954103BC1DE425F96A077410B995891E73E706600B3F3F7B23AC
SHA-512:	E3161717A96BE7C5DC13440E44DF7F4791C53496D20939026689BE160AA04EFF916C08E3F91363158FCC874AD527A18D046A68E3AD2F4FE8DEC9604A155F38EE
Malicious:	**true**
Preview:	..`....H

C:\Users\user\AppData\Roaming\dihsw\chmac.exe	
Process:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	663115
Entropy (8bit):	5.508570188450402
Encrypted:	false
SSDEEP:	6144:lwq9sUW6UzgZb6uxaKHEMiYKpgss9N2zy:6UZYgxc5NYKCr7
MD5:	D272E884F59FF9D7921619F88766709D
SHA1:	B9013DCFFC28E174C1CB7D81FD46B6463B4FF579
SHA-256:	94A00E5D13EEBC1A99DD48E2D9F9CB48935C424C6BD58AB9F6D78FF0CAA36506
SHA-512:	EB8A351EB547A359F246B6E82B4794AEF31E2A350043116965E636A7A69583621C1EE2A5381079A1815A7489BFADC2FC3962AE74CBDF523A4F6E6E7E2379D9C2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 42%
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):	5.508570188450402
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:	G2M8C76V_INV0ICE_RECEIPT.exe
File size:	663115
MD5:	d272e884f59ff9d7921619f88766709d
SHA1:	b9013dcffc28e174c1cb7d81fd46b6463b4ff579
SHA256:	94a00e5d13eebc1a99dd48e2d9f9cb48935c424c6bd58ab9f6d78ff0caa36506
SHA512:	eb8a351eb547a359f246b6e82b4794aef31e2a350043116965e636a7a69583621c1ee2a5381079a1815a7489bfadc2fc3962ae74cbdf523a4f6e6e7e2379d9c2
SSDEEP:	6144:lwq9sUW6UzgZb6uxaKHEMiYKpgss9N2zy:6UZYgxc5NYKCr7
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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
01/13/22-15:32:22.405814	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57875	8.8.8.8	192.168.2.3
01/13/22-15:32:35.830669	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
01/13/22-15:32:48.402158	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60784	8.8.8.8	192.168.2.3
01/13/22-15:32:54.892461	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51143	8.8.8.8	192.168.2.3
01/13/22-15:33:01.332628	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56009	8.8.8.8	192.168.2.3
01/13/22-15:33:07.691280	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55102	8.8.8.8	192.168.2.3
01/13/22-15:33:13.938372	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49559	8.8.8.8	192.168.2.3
01/13/22-15:33:27.058039	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60352	8.8.8.8	192.168.2.3
01/13/22-15:33:47.081904	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64367	8.8.8.8	192.168.2.3
01/13/22-15:34:12.542040	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63456	8.8.8.8	192.168.2.3
01/13/22-15:34:18.907708	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58540	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 15:32:22.209491968 CET	192.168.2.3	8.8.8.8	0x4721	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:28.565608978 CET	192.168.2.3	8.8.8.8	0x8fea	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 15:32:35.717637062 CET	192.168.2.3	8.8.8.8	0xdeca	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:41.991347075 CET	192.168.2.3	8.8.8.8	0x4167	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:48.289732933 CET	192.168.2.3	8.8.8.8	0x4bf8	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:54.779721975 CET	192.168.2.3	8.8.8.8	0x7c96	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:01.219548941 CET	192.168.2.3	8.8.8.8	0x8b00	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:07.577388048 CET	192.168.2.3	8.8.8.8	0x7c76	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:13.824532986 CET	192.168.2.3	8.8.8.8	0x4c89	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:20.093357086 CET	192.168.2.3	8.8.8.8	0x847	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:26.943756104 CET	192.168.2.3	8.8.8.8	0x9ddc	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:33.189743996 CET	192.168.2.3	8.8.8.8	0x2b96	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:39.395334959 CET	192.168.2.3	8.8.8.8	0x5a8	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:46.968370914 CET	192.168.2.3	8.8.8.8	0xff75	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:53.528749943 CET	192.168.2.3	8.8.8.8	0x5d02	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:59.952053070 CET	192.168.2.3	8.8.8.8	0x491c	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:34:06.225054026 CET	192.168.2.3	8.8.8.8	0x779a	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:34:12.427901983 CET	192.168.2.3	8.8.8.8	0x2f7	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 13, 2022 15:34:18.793152094 CET	192.168.2.3	8.8.8.8	0x890f	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 15:32:22.405813932 CET	8.8.8.8	192.168.2.3	0x4721	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:28.585058928 CET	8.8.8.8	192.168.2.3	0x8fea	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:35.830668926 CET	8.8.8.8	192.168.2.3	0xdeca	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:42.010797024 CET	8.8.8.8	192.168.2.3	0x4167	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:48.402158022 CET	8.8.8.8	192.168.2.3	0x4bf8	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:32:54.892461061 CET	8.8.8.8	192.168.2.3	0x7c96	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:01.332628012 CET	8.8.8.8	192.168.2.3	0x8b00	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:07.691279888 CET	8.8.8.8	192.168.2.3	0x7c76	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:13.938371897 CET	8.8.8.8	192.168.2.3	0x4c89	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:20.112741947 CET	8.8.8.8	192.168.2.3	0x847	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:27.058038950 CET	8.8.8.8	192.168.2.3	0x9ddc	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:33.209614038 CET	8.8.8.8	192.168.2.3	0x2b96	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 15:33:39.414510965 CET	8.8.8.8	192.168.2.3	0x5a8	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:47.081903934 CET	8.8.8.8	192.168.2.3	0xff75	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:53.548517942 CET	8.8.8.8	192.168.2.3	0x5d02	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:33:59.971908092 CET	8.8.8.8	192.168.2.3	0x491c	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:34:06.244513035 CET	8.8.8.8	192.168.2.3	0x779a	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:34:12.542040110 CET	8.8.8.8	192.168.2.3	0x2f7	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 13, 2022 15:34:18.907707930 CET	8.8.8.8	192.168.2.3	0x890f	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: G2M8C76V_INV0ICE_RECEIPT.exe PID: 6964 Parent PID: 5748

General

Start time:	15:32:13
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe"
Imagebase:	0x400000
File size:	663115 bytes
MD5 hash:	D272E884F59FF9D7921619F88766709D
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: 00000000.00000002.297135620.00000000030A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.297135620.00000000030A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.297135620.00000000030A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.297135620.00000000030A0000.00000004.00000001.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: G2M8C76V_INV0ICE_RECEIPT.exe PID: 7092 Parent PID: 6964

General

Start time:	15:32:15
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\G2M8C76V_INV0ICE_RECEIPT.exe"
Imagebase:	0x400000
File size:	663115 bytes
MD5 hash:	D272E884F59FF9D7921619F88766709D
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: 00000003.00000001.294779978.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000001.294779978.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000001.294779978.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.293187290.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.293187290.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.293187290.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.294042312.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.294042312.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.294042312.0000000000414000.00000040.00000001.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: 6288 Parent PID: 3352

General

Start time:	15:32:25
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:	663115 bytes
MD5 hash:	D272E884F59FF9D7921619F88766709D
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: 0000000D.00000002.327158537.0000000003000000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.327158537.0000000003000000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.327158537.0000000003000000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.327158537.0000000003000000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 42%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: chmac.exe PID: 6556 Parent PID: 6288

General

Start time:	15:32:27
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:	663115 bytes
MD5 hash:	D272E884F59FF9D7921619F88766709D
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: 0000000E.00000002.341257135.0000000003731000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.341257135.0000000003731000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.341257135.0000000003731000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.322700795.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.322700795.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.322700795.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.323810648.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.323810648.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.323810648.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.341406619.0000000004832000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.341406619.0000000004832000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.341406619.0000000004832000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.341081024.0000000002260000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.341081024.0000000002260000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.341081024.0000000002260000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.341081024.0000000002260000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.340666322.00000000004F4000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.340666322.00000000004F4000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.340666322.00000000004F4000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.340553109.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.340553109.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.340553109.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.340553109.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.341299575.000000000376A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.341299575.000000000376A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.341227508.000000000273E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000001.325215386.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000001.325215386.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000001.325215386.0000000000414000.00000040.00020000.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: 6760 Parent PID: 3352

General

Start time:	15:32:34
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:	663115 bytes
MD5 hash:	D272E884F59FF9D7921619F88766709D
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: 0000000F.00000002.344485087.0000000002540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.344485087.0000000002540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.344485087.0000000002540000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.344485087.0000000002540000.00000004.00000001.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: 6820 Parent PID: 6760

General

Start time:	15:32:36
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:	663115 bytes
MD5 hash:	D272E884F59FF9D7921619F88766709D
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: 00000010.00000002.359331974.00000000024B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.359331974.00000000024B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.359331974.00000000024B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.359331974.00000000024B0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.358998677.0000000000644000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.358998677.0000000000644000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.358998677.0000000000644000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.339547057.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.339547057.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.339547057.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000001.342024233.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000001.342024233.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000001.342024233.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.359590843.00000000038E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.359590843.00000000038E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.359590843.00000000038E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.341018876.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.341018876.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.341018876.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.359549562.00000000028EE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.358899493.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.358899493.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.358899493.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.358899493.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.359622615.000000000391A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.359622615.000000000391A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.359413916.0000000002502000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.359413916.0000000002502000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.359413916.0000000002502000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis