ID: 451838
Sample Name:
kw7HGENm1D.exe
Cookbook: default.jbs
Time: 12:11:10
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

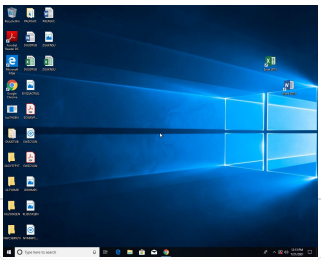
Windows Analysis Report kw7HGENm1D.exe

Overview

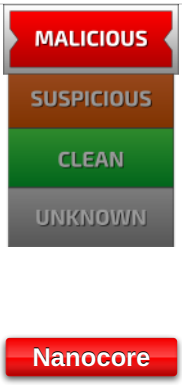
General Information

Sample Name:	kw7HGENm1D.exe
Analysis ID:	451838
MD5:	a854bd1a3ff6d35..
SHA1:	b8de8cb81adbb8..
SHA256:	8fb35304f24a634..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

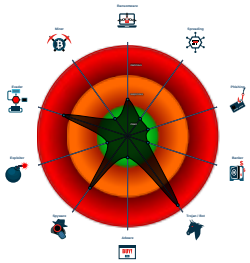


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- kw7HGENm1D.exe (PID: 1700 cmdline: 'C:\Users\user\Desktop\kw7HGENm1D.exe' MD5: A854BD1A3FF6D359A5E2E76154892444)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "39997603-c9cb-4099-abed-49c0195a",
  "Group": "Old",
  "Domain1": "newhost.publicvm.com",
  "Domain2": "backupnewhost.duckdns.org",
  "Port": 9911,
  "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

Initial Sample

Source	Rule	Description	Author	Strings
kw7HGENm1D.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xcafd:$x1: NanoCore.ClientPluginHost • 0xcb34:$x1: NanoCore.ClientPluginHost • 0xdddf:$x1: NanoCore.ClientPluginHost • 0xde13:$x1: NanoCore.ClientPluginHost • 0xdef6:$x1: NanoCore.ClientPluginHost • 0xdf30:$x1: NanoCore.ClientPluginHost • 0xdf6e:$x1: NanoCore.ClientPluginHost • 0xdfa7:$x1: NanoCore.ClientPluginHost • 0xe335:$x1: NanoCore.ClientPluginHost • 0xcb17:$x2: IClientNetworkHost • 0xcb4e:$x2: IClientNetworkHost • 0xe322:$x2: IClientNetworkHost
kw7HGENm1D.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd349:$x1: NanoCore Client.exe • 0xcafd:$x2: NanoCore.ClientPluginHost • 0xcb34:$x2: NanoCore.ClientPluginHost • 0xdddf:$x2: NanoCore.ClientPluginHost • 0xde13:$x2: NanoCore.ClientPluginHost • 0xdef6:$x2: NanoCore.ClientPluginHost • 0xdf30:$x2: NanoCore.ClientPluginHost • 0xdf6e:$x2: NanoCore.ClientPluginHost • 0xdfa7:$x2: NanoCore.ClientPluginHost • 0xe335:$x2: NanoCore.ClientPluginHost • 0xcb9d:$s1: PluginCommand • 0xcb85:$s2: FileCommand • 0xe187:$s3: PipeExists • 0xcaf1:$s4: PipeCreated • 0xe30f:$s5: IClientLoggingHost
kw7HGENm1D.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
kw7HGENm1D.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xcafd:$a: NanoCore • 0xcb34:$a: NanoCore • 0xcf6f:$a: NanoCore • 0xd349:$a: NanoCore • 0xd785:$a: NanoCore • 0xdddf:$a: NanoCore • 0xde13:$a: NanoCore • 0xdef6:$a: NanoCore • 0xdf30:$a: NanoCore • 0xdf6e:$a: NanoCore • 0xdfa7:$a: NanoCore • 0xe22c:$a: NanoCore • 0xe335:$a: NanoCore • 0xcb06:$b: ClientPlugin • 0xcb3d:$b: ClientPlugin • 0xd78e:$b: ClientPlugin • 0xdde8:$b: ClientPlugin • 0xde1c:$b: ClientPlugin • 0xdeff:$b: ClientPlugin • 0xdf39:$b: ClientPlugin • 0xdf77:$b: ClientPlugin

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.514043603.0000000005EE0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
00000000.00000002.514043603.0000000005EE0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
00000000.00000002.514025811.0000000005ED0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
00000000.00000002.514025811.0000000005ED0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
00000000.00000002.511088441.00000000039C0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x5d90a:$a: NanoCore • 0x5d933:$a: NanoCore • 0x827f6:$a: NanoCore • 0x8280e:$a: NanoCore • 0x82837:$a: NanoCore • 0x92dc1:$a: NanoCore • 0x9374c:$a: NanoCore • 0x5d913:$b: ClientPlugin • 0x5d93c:$b: ClientPlugin • 0x82525:$b: ClientPlugin • 0x8253e:$b: ClientPlugin • 0x8256e:$b: ClientPlugin • 0x82817:$b: ClientPlugin • 0x82840:$b: ClientPlugin • 0x92dca:$b: ClientPlugin • 0x93755:$b: ClientPlugin • 0x95b0a:$b: ClientPlugin • 0x5d844:$c: ProjectData • 0x8270d:$c: ProjectData • 0x7dbf5:$e: KeepAlive • 0x924b7:$g: LogClientMessage
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.kw7HGENm1D.exe.4bf0000.16.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0.2.kw7HGENm1D.exe.4bf0000.16.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0.2.kw7HGENm1D.exe.4bf0000.16.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.kw7HGENm1D.exe.4bc0000.14.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
0.2.kw7HGENm1D.exe.4bc0000.14.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 94 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:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

Detected Nanocore Rat

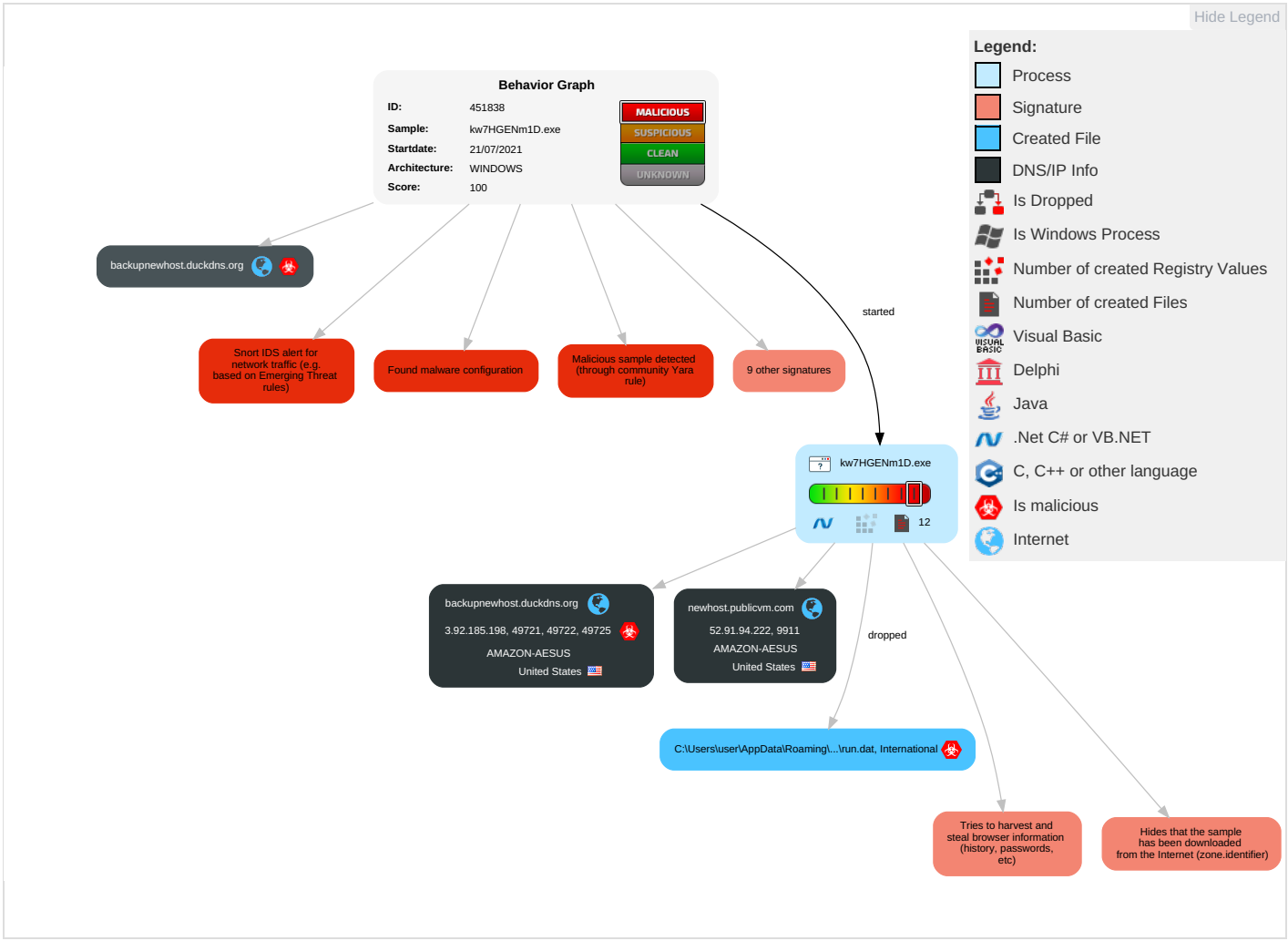
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Ea Ins Ne Cc
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Process Injection 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 4	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Standard Port 1	Ex Tr Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SI Sw

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Ma De Cc
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	Application Layer Protocol 2 1	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dc Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rc Ba

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
kw7HGENm1D.exe	63%	Virustotal		Browse
kw7HGENm1D.exe	60%	Metadefender		Browse
kw7HGENm1D.exe	89%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
kw7HGENm1D.exe	100%	Avira	HEUR/AGEN.1108376	
kw7HGENm1D.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.kw7HGENm1D.exe.4bf0000.16.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.kw7HGENm1D.exe.80000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
0.0.kw7HGENm1D.exe.80000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
backupnewhost.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
newhost.publicvm.com	52.91.94.222	true	false		high
backupnewhost.duckdns.org	3.92.185.198	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
newhost.publicvm.com	false		high
backupnewhost.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.91.94.222	newhost.publicvm.com	United States		14618	AMAZON-AESUS	false
3.92.185.198	backupnewhost.duckdns.org	United States		14618	AMAZON-AESUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451838
Start date:	21.07.2021
Start time:	12:11:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kw7HGENm1D.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/5@16/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.1%) • Quality average: 23.6% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 100% • 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
12:12:05	API Interceptor	1089x Sleep call for process: kw7HGENm1D.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3.92.185.198	CM45.vbs	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	TFG18FA4eD	Get hash	malicious	Browse	• 44.214.154.33
	StyBaUxNYq	Get hash	malicious	Browse	• 52.73.216.92
	qgQgEjI283	Get hash	malicious	Browse	• 100.24.228.158
	jhUxzb7jPW	Get hash	malicious	Browse	• 34.205.150.10
	DDA9.dll	Get hash	malicious	Browse	• 52.20.197.7
	1.dll	Get hash	malicious	Browse	• 3.211.138.232
	4fZX8fJwHn.dll	Get hash	malicious	Browse	• 54.235.190.106
	lpaBPnb1OB.exe	Get hash	malicious	Browse	• 54.243.175.83
	v6clgzEGCb	Get hash	malicious	Browse	• 34.237.123.218
	TNT Shipment.exe	Get hash	malicious	Browse	• 3.208.234.55
	sap7ltEdFx	Get hash	malicious	Browse	• 44.201.155.123
	Dvf7OP92yJ	Get hash	malicious	Browse	• 174.129.61.100
	Vk3A1yJJMg	Get hash	malicious	Browse	• 44.221.179.16
	a1sMR3Vj8o	Get hash	malicious	Browse	• 34.237.211.216
	IMQ74zpulc.exe	Get hash	malicious	Browse	• 3.223.115.185
	Af1Fnq4I4G	Get hash	malicious	Browse	• 100.25.242.76
	r6hA4B4FqS	Get hash	malicious	Browse	• 44.221.167.150
	8wzyljMmmn	Get hash	malicious	Browse	• 34.202.220.187
	appointment letter.xlsx	Get hash	malicious	Browse	• 23.21.157.88

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FN0ZF2Nm21	Get hash	malicious	Browse	• 54.24.234.10
AMAZON-AESUS	TFG18FA4eD	Get hash	malicious	Browse	• 44.214.154.33
	StyBaUxNYq	Get hash	malicious	Browse	• 52.73.216.92
	qgQgEjI283	Get hash	malicious	Browse	• 100.24.228.158
	jhUxzb7jPW	Get hash	malicious	Browse	• 34.205.150.10
	DDA9.dll	Get hash	malicious	Browse	• 52.20.197.7
	1.dll	Get hash	malicious	Browse	• 3.211.138.232
	4fZX8fJwHn.dll	Get hash	malicious	Browse	• 54.235.190.106
	lpaBPnb1OB.exe	Get hash	malicious	Browse	• 54.243.175.83
	v6clgzEGCb	Get hash	malicious	Browse	• 34.237.123.218
	TNT Shipment.exe	Get hash	malicious	Browse	• 3.208.234.55
	sap7ltEdFx	Get hash	malicious	Browse	• 44.201.155.123
	Dvf7OP92yJ	Get hash	malicious	Browse	• 174.129.61.100
	Vk3A1yJJMg	Get hash	malicious	Browse	• 44.221.179.16
	a1sMR3Vj8o	Get hash	malicious	Browse	• 34.237.211.216
	IMQ74zpulc.exe	Get hash	malicious	Browse	• 3.223.115.185
	Af1Fnq4I4G	Get hash	malicious	Browse	• 100.25.242.76
	r6hA4B4FqS	Get hash	malicious	Browse	• 44.221.167.150
	8wzyljMmmn	Get hash	malicious	Browse	• 34.202.220.187
	appointment letter.xlsx	Get hash	malicious	Browse	• 23.21.157.88
	FN0ZF2Nm21	Get hash	malicious	Browse	• 54.24.234.10

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\kw7HGENm1D.exe
File Type:	data
Category:	dropped
Size (bytes):	320
Entropy (8bit):	6.76696567289067
Encrypted:	false
SSDEEP:	6:nprYhSjkONZdGzzG31sV2sS4Ct0r2xprYhSjkONZdGzzG31sV2sS4Ct0r29:npbjkONZdGnmgTS4k0qxpbjkONZdGnmJ
MD5:	FEB350949251AC8F3E7783A2BDE88A51
SHA1:	82FE012F0CC9CF457701EC6DDE99AF73BD73B931
SHA-256:	A32EA0E8DC38655BAC2BA4332C1A231D2B012CE638602F1826B220BA4D91CA61
SHA-512:	7E05DD0845D27D3493728F419506098FE15D17B8B96D7F305A6A30E56B17FAF9FBBE2767CC8B1510274503343DDCC789CB1E275CEF6EA45631AFABD2C40463E
Malicious:	false
Reputation:	low
Preview:	...L=..+.[.1u.Pp.L.*j.m.2FL'7..[..|p.W.i0..QR...6d1.....6~\./.o<..MyFP...A.Rlb....k.CD.S.....P...FK.....81....^..P.w.. ...z`c.=.@.....G..7....n..)..s..O....L=..+.[.1u.Pp.L.*j.m.2FL'7..[..|p.W.i0..QR...6d1.....6~\./.o<..MyFP...A.Rlb....k.CD.S.....P...FK.....81....^..P.w.. ...z`c.=.@.....G..7....n..)..s..O.

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

Process:	C:\Users\user\Desktop\kw7HGENm1D.exe
File Type:	International EBCDIC text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:njp8:nje
MD5:	26AA48EDF508A0DE24C4A8A90EC10DDD
SHA1:	62B2BB7EFED4F798F6665296A329CB61F3AA85E4
SHA-256:	04C2D74AAAF3E89E878078F9B94E1CEDE00C5E12B30BF02A86C2A1172D694868
SHA-512:	191AA80A2D46FD437F5EFD0CD54C9AAE49F6CBB08F139D362FDE924E9227A5842CA3E6B828ADF56450ED9E6F3AF074D0763893DFCA1EB2D58E45F54E395867C

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Malicious:	**true**
Reputation:	low
Preview:	..fm{L.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\kw7HGENm1D.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\kw7HGENm1D.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDlfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\kw7HGENm1D.exe
File Type:	data
Category:	dropped
Size (bytes):	379672
Entropy (8bit):	**7.999528303288865**
Encrypted:	**true**
SSDEEP:	6144:K+3c0wsFFUOVpzvbpRTELXdC53fz1TQdDjZvW+ZQJ03SDjCkI7Nh07MyOFQ9wv2T:ir0bp7PRZcdnZ++Zj3IjKhjOSv9KFBH
MD5:	543352056C5CB25E9BC2BDEAF2BBF9E2
SHA1:	2D1E2BA09C295FB6631F7EDCD3280894FE7D5125
SHA-256:	11227762F426CC8FA6FF700328732AA87A44807AA7C65FA6D97FDB47917CF8F6
SHA-512:	53DC5864B019D6BE0588D8CC9055414A933BA6923E572CB1AE3DE6848ED67FC65AA237C94F6397387C2555E84C88EE38D0B7BF7F4958C351683EF324D2874315
Malicious:	false
Reputation:	low
Preview:	E..v..}3...$..n).E...I.2HbzR.....,..T.7....A.Qy.?9AM>..Q..O.Yr.,...5...X_...;?..!....?.....b....N..<.}/0.E.....{9.....~O.x.^.a..1a.@....`4qZ....H...AWt]..@...w.v.....^A..<X..TQ ...aO..R..z`Xg..@..C...c.....+..]...b.Y....!.O.!c8V+4..zl.hEV.. }.*.wq.K..v @.....f..y.Ex.#*;...P{.Z.....M.4.....7...7..nj.<.|...:.....v.#...{....V,#S..R]~m=..$.....0...}y3.e...V. .@@....K.e.....p..$<0V...$g.<).w..#..vLL.\.Y.)}.....[.....M[C..H..n|F..e.5.C.....7)..r?!.n...*..k.....Ny...rY..Q.....$J|..o#....w..>.....;(.J}.....V..E..m*..5XLUi y.[[.....rW.L ow../...9G...g..y._.WAu.j...,...}.3.....U.B.y.'..P...:.fX.&.N....#.....W..GTEC..u.I)Et...>..5Fs.r2.Jk.....>.u.....D..r.P..;.:..q.O.....Z..... G5~Hk.M..t.T.....[.`...q1..q.....\...s...../..@\..iQK ..E&..e.*.0..l....@.bR...ww:..jG...2Z...v.H..=.8...w.J..-F?W.)...S..u..MIM`L...C...-..f...IK....].eE8.6#`.5.B.....E.q+.....(}.o..c....n]..H.v.. ....z..<C.....Q]...,..O....

Static File Info

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.324667002820176
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	kw7HGENm1D.exe
File size:	160768
MD5:	a854bd1a3ff6d359a5e2e76154892444
SHA1:	b8de8cb81adbb8cc5456a2100ffd3502548b0c2c
SHA256:	8fb35304f24a6348adbd96f2ece69cdc23aa2442cfe28ca910ee31b48fd43632
SHA512:	ebb2d7a7b43f826ddf84aa6374e2c006fdbc2fb8aa924f485b762546eca349f889bb2db50190ca80755741a15542a90c3b0ff035e354c7186fc24c13a7807b19
SSDEEP:	3072:2JEZzJZ5WY+apEbTmFxjpcJslEjqZ4UHtbrObVeHCtEGMyVuz5rMRyJJG+pXSPLE:HZT5TbjiJslEjqZ4UHtbYVehjauz5+Ct
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`.....1... ...@....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41312e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x11134	0x11200	False	0.452953923358	data	5.6930506473	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x14000	0x15da0	0x15e00	False	0.999698660714	data	7.9977388881	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2a000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/21/21-12:12:59.033903	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:05.270177	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:11.269344	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:17.441073	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:23.621332	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:29.585150	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:35.610599	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:41.778497	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:52.234768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	9911	192.168.2.5	3.92.185.198
07/21/21-12:13:59.650035	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	9911	192.168.2.5	3.92.185.198
07/21/21-12:14:05.853550	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	9911	192.168.2.5	3.92.185.198
07/21/21-12:14:11.894029	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	9911	192.168.2.5	3.92.185.198

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 12:12:06.695765018 CEST	192.168.2.5	8.8.8.8	0x6c37	Standard query (0)	newhost.publicvm.com	A (IP address)	IN (0x0001)
Jul 21, 2021 12:12:24.108674049 CEST	192.168.2.5	8.8.8.8	0x6d6d	Standard query (0)	newhost.publicvm.com	A (IP address)	IN (0x0001)
Jul 21, 2021 12:12:41.589500904 CEST	192.168.2.5	8.8.8.8	0x9aff	Standard query (0)	newhost.publicvm.com	A (IP address)	IN (0x0001)
Jul 21, 2021 12:12:58.755163908 CEST	192.168.2.5	8.8.8.8	0xe1ea	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:05.041157007 CEST	192.168.2.5	8.8.8.8	0x7169	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:11.152848959 CEST	192.168.2.5	8.8.8.8	0xa891	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:17.289640903 CEST	192.168.2.5	8.8.8.8	0x4059	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 12:13:23.504897118 CEST	192.168.2.5	8.8.8.8	0xb620	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:29.468622923 CEST	192.168.2.5	8.8.8.8	0xe44c	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:35.474404097 CEST	192.168.2.5	8.8.8.8	0xbc47	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:41.555166006 CEST	192.168.2.5	8.8.8.8	0x4e8a	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:47.726733923 CEST	192.168.2.5	8.8.8.8	0x8e5a	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:52.119225979 CEST	192.168.2.5	8.8.8.8	0x2b2f	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:59.396620035 CEST	192.168.2.5	8.8.8.8	0xbf77	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:14:05.612689018 CEST	192.168.2.5	8.8.8.8	0xcad5	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 12:14:11.677594900 CEST	192.168.2.5	8.8.8.8	0xa7c2	Standard query (0)	backupnewhost.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 12:12:06.822557926 CEST	8.8.8.8	192.168.2.5	0x6c37	No error (0)	newhost.publicvm.com		52.91.94.222	A (IP address)	IN (0x0001)
Jul 21, 2021 12:12:24.249049902 CEST	8.8.8.8	192.168.2.5	0x6d6d	No error (0)	newhost.publicvm.com		52.91.94.222	A (IP address)	IN (0x0001)
Jul 21, 2021 12:12:41.602220058 CEST	8.8.8.8	192.168.2.5	0x9aff	No error (0)	newhost.publicvm.com		52.91.94.222	A (IP address)	IN (0x0001)
Jul 21, 2021 12:12:58.881452084 CEST	8.8.8.8	192.168.2.5	0xe1ea	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:05.165946960 CEST	8.8.8.8	192.168.2.5	0x7169	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:11.166309118 CEST	8.8.8.8	192.168.2.5	0xa891	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:17.303548098 CEST	8.8.8.8	192.168.2.5	0x4059	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:23.518405914 CEST	8.8.8.8	192.168.2.5	0xb620	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:29.481996059 CEST	8.8.8.8	192.168.2.5	0xe44c	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:35.486541033 CEST	8.8.8.8	192.168.2.5	0xbc47	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:41.674238920 CEST	8.8.8.8	192.168.2.5	0x4e8a	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:47.739984989 CEST	8.8.8.8	192.168.2.5	0x8e5a	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:52.131959915 CEST	8.8.8.8	192.168.2.5	0x2b2f	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:13:59.520096064 CEST	8.8.8.8	192.168.2.5	0xbf77	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:14:05.725886106 CEST	8.8.8.8	192.168.2.5	0xcad5	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)
Jul 21, 2021 12:14:11.792047024 CEST	8.8.8.8	192.168.2.5	0xa7c2	No error (0)	backupnewhost.duckdns.org		3.92.185.198	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: kw7HGENm1D.exe PID: 1700 Parent PID: 5704

General

Start time:	12:12:04
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\kw7HGENm1D.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\kw7HGENm1D.exe'
Imagebase:	0x80000
File size:	160768 bytes
MD5 hash:	A854BD1A3FF6D359A5E2E76154892444
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.514043603.0000000005EE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.514043603.0000000005EE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.514025811.0000000005ED0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.514025811.0000000005ED0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.511088441.00000000039C0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.514088521.0000000005F20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.514088521.0000000005F20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.236906939.0000000000082000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.236906939.0000000000082000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.512440128.0000000004BC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.512440128.0000000004BC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.354611004.0000000003ACC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.513862961.0000000005E40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.513862961.0000000005E40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.510127578.0000000003689000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.512499976.0000000004BF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.512499976.0000000004BF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.512499976.0000000004BF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.513888087.0000000005E50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.513888087.0000000005E50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.504244186.0000000000082000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.504244186.0000000000082000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.513910421.0000000005E60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.513910421.0000000005E60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.508012570.0000000002631000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.513957780.0000000005E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.513957780.0000000005E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.514007279.0000000005EC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.514007279.0000000005EC0000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis