ID: 494994
Sample Name: manager.exe
Cookbook: default.jbs
Time: 09:45:19
Date: 01/10/2021
Version: 33.0.0 White Diamond

Table of Contents

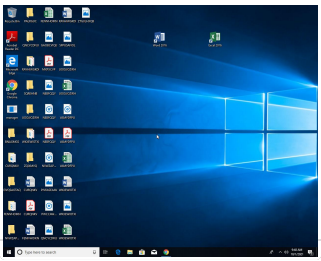
Windows Analysis Report manager.exe

Overview

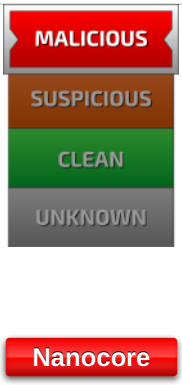
General Information

Sample Name:	manager.exe
Analysis ID:	494994
MD5:	1479371ef0752f0..
SHA1:	3bf6809d0987cd8.
SHA256:	183923330057af9.
Infos:	

Most interesting Screenshot:



Detection



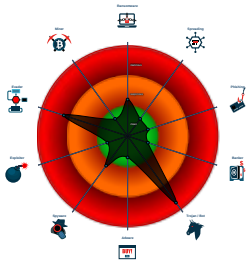
Nanocore

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 / Scanner detection for sub…
- Yara detected Nanocore RAT
- Machine Learning detection for samp…
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- manager.exe (PID: 6836 cmdline: 'C:\Users\user\Desktop\manager.exe' MD5: 1479371EF0752F027661FC1B7748B318)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "69d5e1dd-adbf-4c76-9eba-4ac963b0",
  "Group": "Manager",
  "Domain1": "findmyservice.ignorelist.com",
  "Port": 4001,
  "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
manager.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
manager.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
manager.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
manager.exe	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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.613548998.0000000004E00000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000000.00000002.613548998.0000000004E00000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000000.00000002.613718440.00000000051B0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000000.00000002.613718440.00000000051B0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000000.00000002.613718440.00000000051B0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.manager.exe.51b0000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0.2.manager.exe.51b0000.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0.2.manager.exe.51b0000.7.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.manager.exe.3a42a75.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c50:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c7d:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
0.2.manager.exe.3a42a75.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x23c50:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x24d2b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x23c6a:$s5: IClientLoggingHost
Click to see the 29 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 / Scanner detection for submitted sample

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

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

Remote Access Functionality:

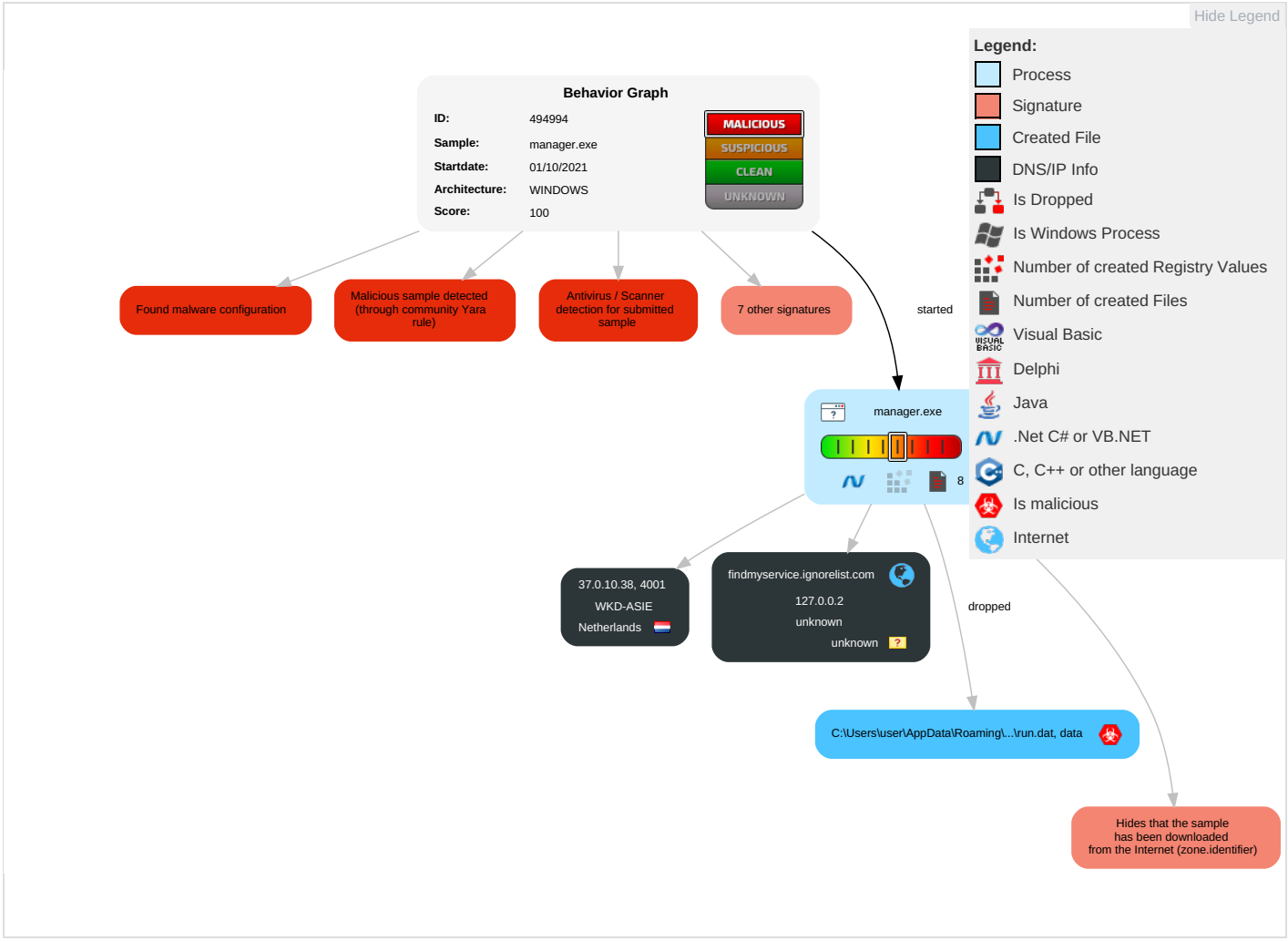
Detected Nanocore Rat

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	Netv Effe
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	Input Capture 1 1	Process Discovery 2	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netw Com
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

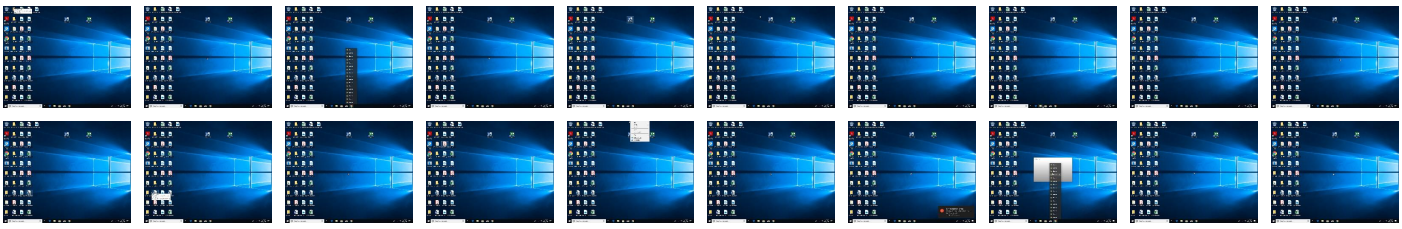
Behavior Graph



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
manager.exe	88%	Virustotal		Browse
manager.exe	86%	Metadefender		Browse
manager.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
manager.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
manager.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.manager.exe.290000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.manager.exe.51b0000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
0.2.manager.exe.290000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
findmyservice.ignorelist.com	127.0.0.2	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
findmyservice.ignorelist.com	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.10.38	unknown	Netherlands		198301	WKD-ASIE	false

Private

IP
127.0.0.2

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	494994
Start date:	01.10.2021
Start time:	09:45:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	manager.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:	17
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@1/1@6/2
EGA Information:	• Successful, ratio: 100%

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

Simulations

Behavior and APIs

Time	Type	Description
09:46:17	API Interceptor	1006x Sleep call for process: manager.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37.0.10.38	manager.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WKD-ASIE	manager.exe	Get hash	malicious	Browse	• 37.0.10.38
	37B2718705E2CDCBE38E2E27173BA95467B68D45187A2.exe	Get hash	malicious	Browse	• 37.0.8.119
	20F43079CF75825C5E909B04F3C0B8BDB2F71BE7477FB.exe	Get hash	malicious	Browse	• 37.0.8.119
	A6A0C59A5F4C53AC5DF74AAE93D700CF287A370505D81.exe	Get hash	malicious	Browse	• 37.0.10.214
	63301A39B93B63ACAB80E0A05B909F733D792C7AE829A.exe	Get hash	malicious	Browse	• 37.0.8.119
	F2F9785308BB396F5EB8C14E746228D3298A5984313EF.exe	Get hash	malicious	Browse	• 37.0.10.214
	3153CAF54366C0DDEDDD293791B8F05EABD7343D9A73C.exe	Get hash	malicious	Browse	• 37.0.8.119
	Circular PSSB Parts Disc Credit Term (Dlr) s.exe	Get hash	malicious	Browse	• 37.0.10.22
	view_2021-09-29_07-17.exe	Get hash	malicious	Browse	• 37.0.8.36
	IznT1D3bT1.exe	Get hash	malicious	Browse	• 37.0.8.154
	T.T.exe	Get hash	malicious	Browse	• 37.0.10.22
	manager.exe	Get hash	malicious	Browse	• 37.0.10.38
	EXTRACTO_SERFINANZA_4295529724698441156_542157354638_25702910368262995_65000377634382740.exe	Get hash	malicious	Browse	• 37.0.10.149
	PPT-0000084510027306.exe	Get hash	malicious	Browse	• 37.0.10.190
	071F6BD61AEF9F209BE1BFB16EF1FB14BD44804FCAB51.exe	Get hash	malicious	Browse	• 37.0.8.119
	2awEYXkQvX.exe	Get hash	malicious	Browse	• 37.0.8.119
	DOCU_SIGN8289292930001028838.PDF.exe	Get hash	malicious	Browse	• 37.0.8.37
	Product List.exe	Get hash	malicious	Browse	• 37.0.8.14
	A4B51BD72DFFD28AD3841217FFEC9E43D21EE3C6F889B.exe	Get hash	malicious	Browse	• 37.0.8.119
	44F3C573B5D6D77D97C2EBF5D4A235DA5AED3A18EB5B7.exe	Get hash	malicious	Browse	• 37.0.8.119

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\manager.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Ffqtn:lWn
MD5:	9B62CE3A1EEDE3F40D94989F6205DEC5
SHA1:	2A90D0264E08BCCF4B5802F4854DE614FADA3010
SHA-256:	EBE4EAF950A638CD915D08F8F92868B77A7534F14BF984B7CBB58F0592193391
SHA-512:	0090E5A0A6246E4568AAFC1DFCD9FF0FF1C8E5182211528B00D161A36B492FFFB1E852862419CAD87BF082EB54C2294B3DEA3B81BCC85C93AAC64DB88181A5(A
Malicious:	**true**
Reputation:	low
Preview:	.....H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.4485585447335865
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:	manager.exe
File size:	207360
MD5:	1479371ef0752f027661fc1b7748b318
SHA1:	3bf6809d0987cd82ec328b7bbdbcc5618743cf38
SHA256:	183923330057af95cedb73d0aa2e7f844dba89df8866995f483be4c5780298b3
SHA512:	cb10d09a5fc39acf2b799534900d0af2196df00123c6bbc485646960da69a0012d9423c60ae2d04687351fee52fc132c48bc62cc109f88588f766f9d977ce6f2
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIi1fO32vT/T6BQ1bxjOhdiinvX:gLV6Bta6dtJmakIM5xfO32vTj19B+1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
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	0x1c798	0x1c800	False	0.594512404057	data	6.59809023975	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15da0	0x15e00	False	0.999810267857	data	7.9978283616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 1, 2021 09:46:18.304255962 CEST	192.168.2.6	8.8.8.8	0x6672	Standard query (0)	findmyservice.ignorelist.com	A (IP address)	IN (0x0001)
Oct 1, 2021 09:46:23.521905899 CEST	192.168.2.6	8.8.8.8	0x87ff	Standard query (0)	findmyservice.ignorelist.com	A (IP address)	IN (0x0001)
Oct 1, 2021 09:46:28.798232079 CEST	192.168.2.6	8.8.8.8	0x72d9	Standard query (0)	findmyservice.ignorelist.com	A (IP address)	IN (0x0001)
Oct 1, 2021 09:47:29.904046059 CEST	192.168.2.6	8.8.8.8	0x5557	Standard query (0)	findmyservice.ignorelist.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 1, 2021 09:47:35.054523945 CEST	192.168.2.6	8.8.8.8	0x94bf	Standard query (0)	findmyserv ice.ignorelist.com	A (IP address)	IN (0x0001)
Oct 1, 2021 09:47:40.144175053 CEST	192.168.2.6	8.8.8.8	0xdf6f	Standard query (0)	findmyserv ice.ignorelist.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 1, 2021 09:46:18.421449900 CEST	8.8.8.8	192.168.2.6	0x6672	No error (0)	findmyserv ice.ignorelist.com		127.0.0.2	A (IP address)	IN (0x0001)
Oct 1, 2021 09:46:23.664788961 CEST	8.8.8.8	192.168.2.6	0x87ff	No error (0)	findmyserv ice.ignorelist.com		127.0.0.2	A (IP address)	IN (0x0001)
Oct 1, 2021 09:46:28.815990925 CEST	8.8.8.8	192.168.2.6	0x72d9	No error (0)	findmyserv ice.ignorelist.com		127.0.0.2	A (IP address)	IN (0x0001)
Oct 1, 2021 09:47:29.917476892 CEST	8.8.8.8	192.168.2.6	0x5557	No error (0)	findmyserv ice.ignorelist.com		127.0.0.2	A (IP address)	IN (0x0001)
Oct 1, 2021 09:47:35.066550970 CEST	8.8.8.8	192.168.2.6	0x94bf	No error (0)	findmyserv ice.ignorelist.com		127.0.0.2	A (IP address)	IN (0x0001)
Oct 1, 2021 09:47:40.157917023 CEST	8.8.8.8	192.168.2.6	0xdf6f	No error (0)	findmyserv ice.ignorelist.com		127.0.0.2	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: manager.exe PID: 6836 Parent PID: 5560

General

Start time:	09:46:16
Start date:	01/10/2021
Path:	C:\Users\user\Desktop\manager.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\manager.exe'
Imagebase:	0x290000
File size:	207360 bytes
MD5 hash:	1479371EF0752F027661FC1B7748B318
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: 00000000.00000002.613548998.0000000004E00000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.613548998.0000000004E00000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.613718440.00000000051B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.613718440.00000000051B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.613718440.00000000051B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.341607342.0000000000292000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.341607342.0000000000292000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.341607342.0000000000292000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.609531824.0000000000292000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.609531824.0000000000292000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.609531824.0000000000292000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.612976062.0000000003A28000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.612976062.0000000003A28000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis