ID: 483429
Sample Name:
01_extracted.exe
Cookbook: default.jbs
Time: 00:26:08
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

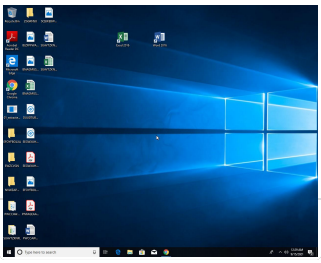
Windows Analysis Report 01_extracted.exe

Overview

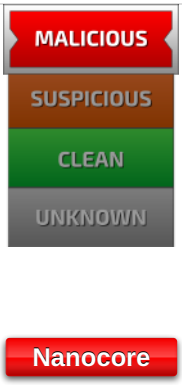
General Information

Sample Name:	01_extracted.exe
Analysis ID:	483429
MD5:	59f356092b9f54b..
SHA1:	252ee78cd15975..
SHA256:	2206669cc770b9..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

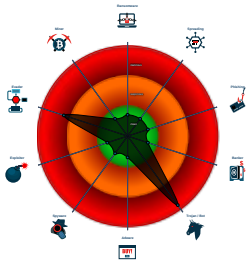


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- 01_extracted.exe (PID: 2392 cmdline: 'C:\Users\user\Desktop\01_extracted.exe' MD5: 59F356092B9F54B4EE5563A2FB8A3255)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "af905a54-91e0-44a6-90a1-2d1125da",
  "Group": "septe123",
  "Domain1": "sunnysept.duckdns.org",
  "Domain2": "sunnysept.duckdns.org",
  "Port": 5500,
  "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
01_extracted.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
01_extracted.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
01_extracted.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
01_extracted.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
00000000.00000000.210003414.000000000262000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.210003414.000000000262000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.210003414.000000000262000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Process Memory Space: 01_extracted.exe PID: 2392	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb485:$x1: NanoCore.ClientPluginHost • 0xb4c2:$x2: IClientNetworkHost • 0xefb3:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x1a039:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Process Memory Space: 01_extracted.exe PID: 2392	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.01_extracted.exe.260000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.0.01_extracted.exe.260000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.0.01_extracted.exe.260000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.0.01_extracted.exe.260000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

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

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

Remote Access Functionality:

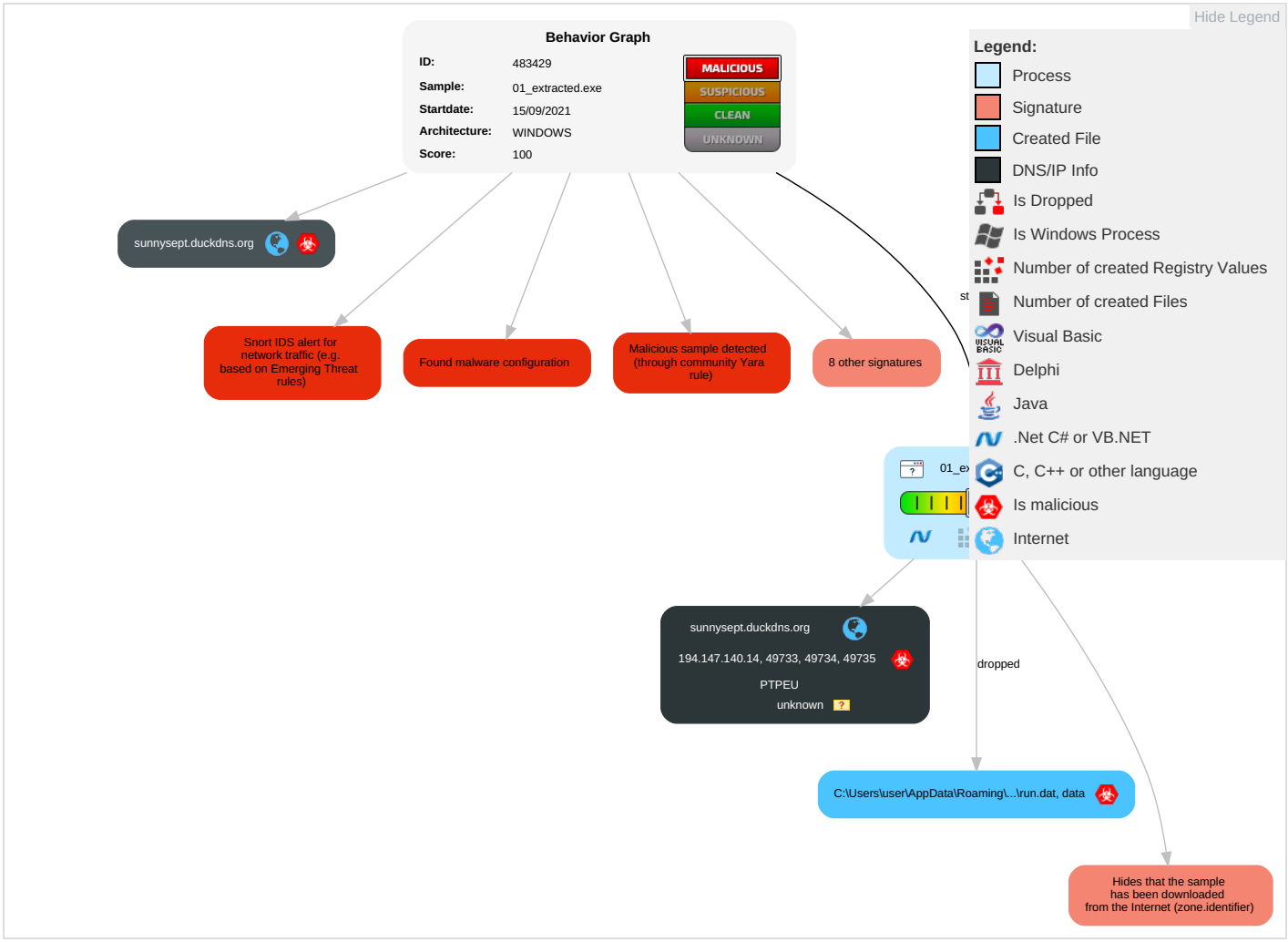
Yara detected Nanocore RAT

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	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 to Redirect Phone Calls/SMS
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	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
01_extracted.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
01_extracted.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.01_extracted.exe.260000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

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

URLs

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

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sunnysept.duckdns.org	194.147.140.14	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
sunnysept.duckdns.org	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.147.140.14	sunnysept.duckdns.org	unknown	?	47285	PTPEU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483429
Start date:	15.09.2021
Start time:	00:26:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	01_extracted.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:	23
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@1/2@22/1
EGA Information:	Failed
HDC Information:	Failed
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
00:27:00	API Interceptor	1046x Sleep call for process: 01_extracted.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sunnysept.duckdns.org	83736354Invoicereceipt.vbs	Get hash	malicious	Browse	• 198.23.251.21

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PTPEU	B4D3E2A30B09D1F2F33476F5234BD7A045973DDBC41A7.exe	Get hash	malicious	Browse	• 194.147.140.8
	18-ITEMS-RECEIPT.vbs	Get hash	malicious	Browse	• 194.147.140.20
	7-Items-receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	9 ITEMS INVOICE RECEIPT.vbs	Get hash	malicious	Browse	• 194.147.140.20
	15 Items Receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	14 Items receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	16 Items receipt.vbs	Get hash	malicious	Browse	• 194.147.140.20
	SPT DRINGENDE BESTELLUNG _876453,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	41-Items-invoice.vbs	Get hash	malicious	Browse	• 194.147.140.20
	Confirmaci#U00f3n del pedido- No HD10103,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	SPT DRINGENDE BESTELLUNG _8764,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	8 Items invoice.vbs	Get hash	malicious	Browse	• 194.147.140.20
	heimatec RFQ 4556_ DRINGEND,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	Confirmarea comenzii noi-4019,pdf.exe	Get hash	malicious	Browse	• 194.147.140.9
	vuaXoDsazg	Get hash	malicious	Browse	• 194.147.142.145
	dsMBH5SmxL	Get hash	malicious	Browse	• 194.147.142.145
	YIupXk5F7b	Get hash	malicious	Browse	• 194.147.142.145
	pvbuEVYCUB	Get hash	malicious	Browse	• 194.147.142.145
	1jTsJsy5b8	Get hash	malicious	Browse	• 194.147.142.145
	fpAHzxlGRn	Get hash	malicious	Browse	• 194.147.142.145

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\01_extracted.exe
File Type:	data
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	24:IQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4jh+K:IknjhUknjhUknjhUknjhUknjhL
MD5:	7BEBBE1F1511163A3243CD8E0C75CC69
SHA1:	216B3AB5D802FA037A6EC5348B189398D8980B3C
SHA-256:	79A130865E9EFFFAA6C2E453942CE87F652681BCD76AAF987318300CAF5E3778
SHA-512:	4DCCB32411DEF72C938022B8675DA50B2DC4CD2C051B1C0377F63D6AAC42FC3D128B0ED580FB88954AB04A9E9EC8D272EBCCF74EB3F136BEF41ADBB845A1 530
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......[.&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......[.&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......[.&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......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\01_extracted.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:c:c
MD5:	315CCD3669C58A3177FFB7D0189A1EEF
SHA1:	678EF06864D26881E2DB1B9511A32B56CF988F3A
SHA-256:	FFA8198F332474004817F0E82E3C209AF881FCDF52F51F30497A6AE6BFB37866
SHA-512:	D9FD615BE3D8AFEC18151D0CE055602C346F1525FD8ECBCA47B6D204FAC13DCD821B385B46DFC39CE5B3BDEFB23D7E75DB6F583505A31CC412F473B1C05E E4E
Malicious:	**true**
Reputation:	low
Preview:	.)5.x.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.446133348432718
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:	01_extracted.exe
File size:	207360
MD5:	59f356092b9f54b4ee5563a2fb8a3255
SHA1:	252ee78cd1597581b9dc14253a77526ef344af38
SHA256:	2206669cc770b99bfdcc44079e5f218a3b4161c7c973f652d6a497a58031bf1d
SHA512:	7043f238357ef4d13c4ebd4c21371173157332547ccf0777594fcdcc566f78f865850a28fabb43ee23f24b26bbf03ed3ee0ea03b299c1565313db623ccbfc128
SSDEEP:	6144:gLV6Bta6dtJmakIM5wq+HjVCuSj2OjrtJrIOXu:gLV6BtpmkNq+DVcH85

General

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	0.594503837719	data	6.5980706265	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	0x15d90	0x15e00	False	0.999732142857	data	7.99777392121	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-00:27:02.076627	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50200	8.8.8.8	192.168.2.3
09/15/21-00:27:02.354546	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:07.400195	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51281	8.8.8.8	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-00:27:07.631437	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:12.383586	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49199	8.8.8.8	192.168.2.3
09/15/21-00:27:12.611541	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:17.744080	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:23.140472	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:28.739254	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:34.478410	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:39.773403	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65110	8.8.8.8	192.168.2.3
09/15/21-00:27:39.998463	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:45.423084	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:50.997919	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	5500	192.168.2.3	194.147.140.14
09/15/21-00:27:56.021163	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:02.027049	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:07.677320	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49563	8.8.8.8	192.168.2.3
09/15/21-00:28:08.684677	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:15.052658	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:21.468840	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:28.077642	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57084	8.8.8.8	192.168.2.3
09/15/21-00:28:28.305043	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:35.011567	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57568	8.8.8.8	192.168.2.3
09/15/21-00:28:35.239451	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:41.718002	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:48.005439	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55435	8.8.8.8	192.168.2.3
09/15/21-00:28:48.231608	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	5500	192.168.2.3	194.147.140.14
09/15/21-00:28:54.654295	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	5500	192.168.2.3	194.147.140.14
09/15/21-00:29:00.711953	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56132	8.8.8.8	192.168.2.3
09/15/21-00:29:00.938829	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	5500	192.168.2.3	194.147.140.14
09/15/21-00:29:07.032341	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	5500	192.168.2.3	194.147.140.14

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 00:27:01.947751045 CEST	192.168.2.3	8.8.8.8	0x369f	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 00:27:07.272417068 CEST	192.168.2.3	8.8.8.8	0x673	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:12.254900932 CEST	192.168.2.3	8.8.8.8	0x55cf	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:17.482837915 CEST	192.168.2.3	8.8.8.8	0x3be6	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:22.885296106 CEST	192.168.2.3	8.8.8.8	0x18e9	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:28.477812052 CEST	192.168.2.3	8.8.8.8	0xc3fb	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:34.172791004 CEST	192.168.2.3	8.8.8.8	0xd60b	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:39.649972916 CEST	192.168.2.3	8.8.8.8	0xd20	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:45.167210102 CEST	192.168.2.3	8.8.8.8	0x7879	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:50.734563112 CEST	192.168.2.3	8.8.8.8	0x7d4f	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:55.767343998 CEST	192.168.2.3	8.8.8.8	0x7772	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:01.768517017 CEST	192.168.2.3	8.8.8.8	0x5cc8	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:07.552164078 CEST	192.168.2.3	8.8.8.8	0x12e5	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:14.785747051 CEST	192.168.2.3	8.8.8.8	0xfdc0	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:21.204571962 CEST	192.168.2.3	8.8.8.8	0x114a	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:27.949857950 CEST	192.168.2.3	8.8.8.8	0xe839	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:34.886750937 CEST	192.168.2.3	8.8.8.8	0x10c6	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:41.456763029 CEST	192.168.2.3	8.8.8.8	0x3859	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:47.879156113 CEST	192.168.2.3	8.8.8.8	0x36fb	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:54.399796963 CEST	192.168.2.3	8.8.8.8	0xd1d0	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:29:00.587172031 CEST	192.168.2.3	8.8.8.8	0x1acf	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)
Sep 15, 2021 00:29:06.781688929 CEST	192.168.2.3	8.8.8.8	0x4c4d	Standard query (0)	sunnysept.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 00:27:02.076627016 CEST	8.8.8.8	192.168.2.3	0x369f	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:07.400194883 CEST	8.8.8.8	192.168.2.3	0x673	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:12.383585930 CEST	8.8.8.8	192.168.2.3	0x55cf	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:17.516397953 CEST	8.8.8.8	192.168.2.3	0x3be6	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:22.912415028 CEST	8.8.8.8	192.168.2.3	0x18e9	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:28.513227940 CEST	8.8.8.8	192.168.2.3	0xc3fb	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:34.251058102 CEST	8.8.8.8	192.168.2.3	0xd60b	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:39.773402929 CEST	8.8.8.8	192.168.2.3	0xd20	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:45.197247028 CEST	8.8.8.8	192.168.2.3	0x7879	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:27:50.770559072 CEST	8.8.8.8	192.168.2.3	0x7d4f	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 00:27:55.794513941 CEST	8.8.8.8	192.168.2.3	0x7772	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:01.800992966 CEST	8.8.8.8	192.168.2.3	0x5cc8	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:07.677320004 CEST	8.8.8.8	192.168.2.3	0x12e5	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:14.822325945 CEST	8.8.8.8	192.168.2.3	0xfdc0	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:21.239867926 CEST	8.8.8.8	192.168.2.3	0x114a	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:28.077641964 CEST	8.8.8.8	192.168.2.3	0xe839	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:35.011567116 CEST	8.8.8.8	192.168.2.3	0x10c6	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:41.491748095 CEST	8.8.8.8	192.168.2.3	0x3859	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:48.005439043 CEST	8.8.8.8	192.168.2.3	0x36fb	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:28:54.427526951 CEST	8.8.8.8	192.168.2.3	0xd1d0	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:29:00.711952925 CEST	8.8.8.8	192.168.2.3	0x1acf	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)
Sep 15, 2021 00:29:06.808100939 CEST	8.8.8.8	192.168.2.3	0x4c4d	No error (0)	sunnysept.duckdns.org		194.147.140.14	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: 01_extracted.exe PID: 2392 Parent PID: 5692

General

Start time:	00:26:59
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\01_extracted.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\01_extracted.exe'
Imagebase:	0x260000
File size:	207360 bytes
MD5 hash:	59F356092B9F54B4EE5563A2FB8A3255
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: 00000000.00000000.210003414.0000000000262000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.210003414.0000000000262000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.210003414.0000000000262000.00000002.00020000.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