ID: 509412
Sample Name:
2FXSF6MXcV.exe
Cookbook: default.jbs
Time: 14:34:06
Date: 26/10/2021
Version: 33.0.0 White Diamond

Table of Contents

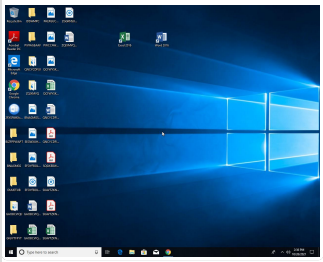
Windows Analysis Report 2FXSF6MXcV.exe

Overview

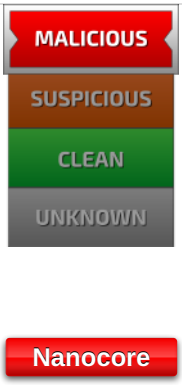
General Information

Sample Name:	2FXSF6MXcV.exe
Analysis ID:	509412
MD5:	e13b24cda6737f1.
SHA1:	b58a2436a4befb5.
SHA256:	f8ee546f04fa175…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



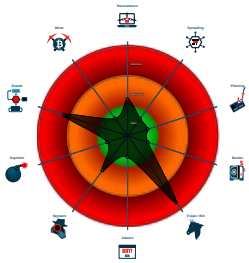
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Drops executable to a common third…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Sigma detected: Suspicious Svchos…
- Machine Learning detection for dropp…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- 2FXSF6MXcV.exe (PID: 6132 cmdline: 'C:\Users\user\Desktop\2FXSF6MXcV.exe' MD5: E13B24CDA6737F13B2DC3F2C20D8823B)
  - svchost.exe (PID: 4936 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - 2FXSF6MXcV.exe (PID: 4936 cmdline: C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe MD5: E13B24CDA6737F13B2DC3F2C20D8823B)
- firefox.exe (PID: 5536 cmdline: 'C:\Users\user\AppData\Roaming\firefox.exe' MD5: E13B24CDA6737F13B2DC3F2C20D8823B)
- firefox.exe (PID: 6312 cmdline: 'C:\Users\user\AppData\Roaming\firefox.exe' MD5: E13B24CDA6737F13B2DC3F2C20D8823B)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "9b8ed064-d4db-4d21-985f-e3763341",
  "Group": "OCT",
  "Domain1": "chongmei33.publicvm.com",
  "Domain2": "chongmei33.publicvm.com",
  "Port": 5569,
  "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
00000013.00000000.410602716.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000013.00000000.410602716.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000013.00000000.410602716.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000013.00000000.411789598.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000013.00000000.411789598.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.0.2FXSF6MXcV.exe.400000.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
19.0.2FXSF6MXcV.exe.400000.6.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:$s5: IClientLoggingHost
19.0.2FXSF6MXcV.exe.400000.6.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
19.0.2FXSF6MXcV.exe.400000.6.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$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
19.2.2FXSF6MXcV.exe.65e4629.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
Click to see the 74 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

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

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

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

Persistence and Installation Behavior:

Drops executable to a common third party application directory

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

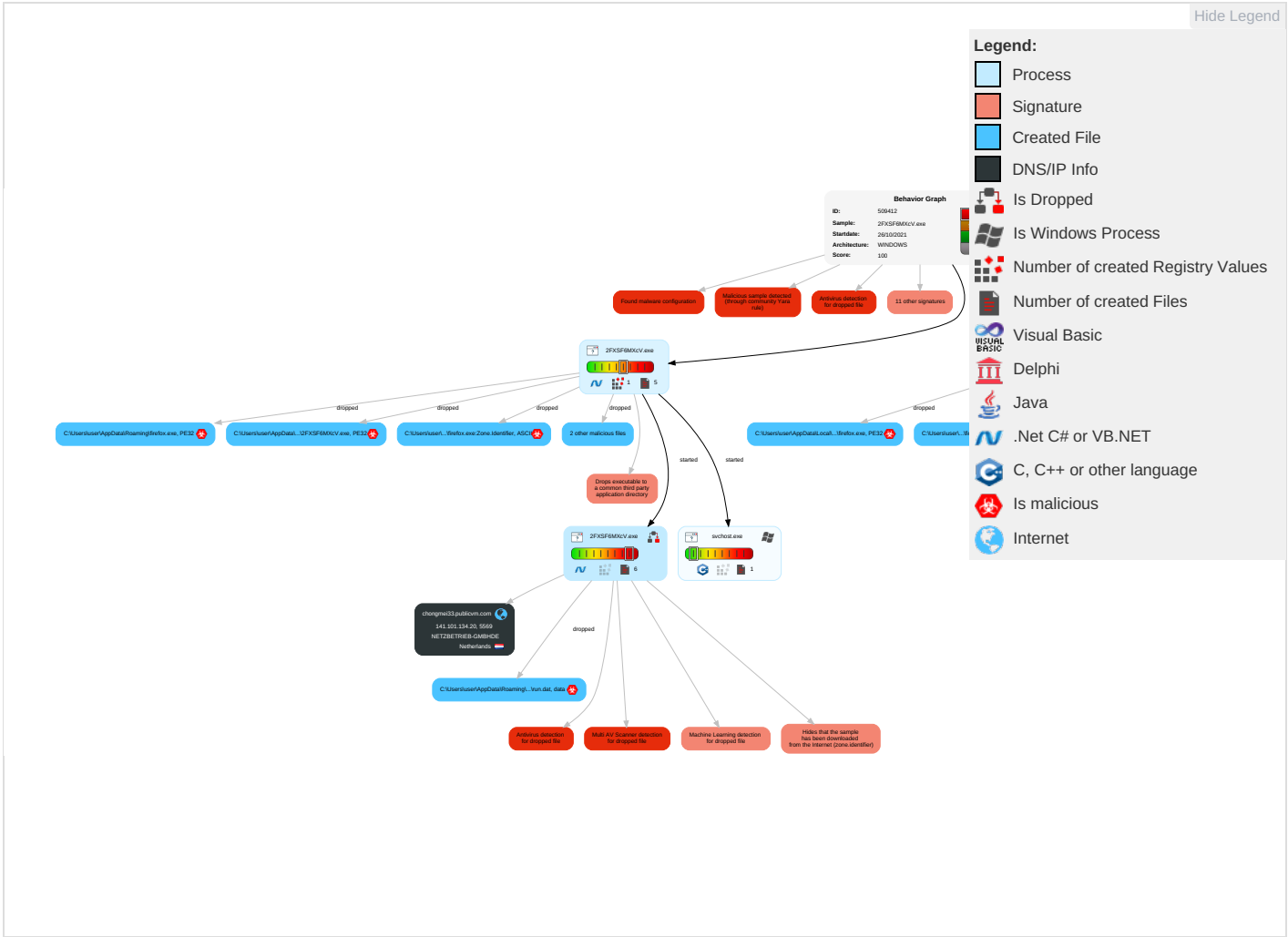
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 1 1	Input Capture 2 1	Security Software Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc

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
2FXSF6MXcV.exe	33%	ReversingLabs	Win32.Keylogger.KeyBase	
2FXSF6MXcV.exe	100%	Avira	TR/Dropper.MSIL.Gen	
2FXSF6MXcV.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\firefox.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Roaming\firefox.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Local\Temp\firefox.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\firefox.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe	33%	ReversingLabs	Win32.Keylogger.KeyBase	
C:\Users\user\AppData\Local\Temp\firefox.exe	33%	ReversingLabs	Win32.Keylogger.KeyBase	
C:\Users\user\AppData\Roaming\firefox.exe	33%	ReversingLabs	Win32.Keylogger.KeyBase	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.2FXSF6MXcV.exe.ce0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.0.2FXSF6MXcV.exe.ff0000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.0.2FXSF6MXcV.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.2FXSF6MXcV.exe.ff0000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
24.0.firefox.exe.d80000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.2.2FXSF6MXcV.exe.65e0000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
19.0.2FXSF6MXcV.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.2FXSF6MXcV.exe.ff0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
24.2.firefox.exe.d80000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.0.2FXSF6MXcV.exe.ff0000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.2.2FXSF6MXcV.exe.ff0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.0.2FXSF6MXcV.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.2FXSF6MXcV.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.2FXSF6MXcV.exe.ff0000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.0.2FXSF6MXcV.exe.ff0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
21.0.firefox.exe.dd0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.0.2FXSF6MXcV.exe.ff0000.13.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.0.2FXSF6MXcV.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.2FXSF6MXcV.exe.ff0000.11.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
19.2.2FXSF6MXcV.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.2FXSF6MXcV.exe.ff0000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.2.2FXSF6MXcV.exe.ce0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chongmei33.publicvm.com	141.101.134.20	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
chongmei33.publicvm.com	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
141.101.134.20	chongmei33.publicvm.com	Netherlands		201011	NETZBETRIEB-GMBHDE	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509412
Start date:	26.10.2021
Start time:	14:34:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2FXSF6MXcV.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/8@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 52.9% • Quality standard deviation: 23.7%
HCA Information:	• Successful, ratio: 82% • 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
14:35:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run firefox "C:\Users\user\AppData\Roaming\firefox.exe"
14:36:03	API Interceptor	497x Sleep call for process: 2FXSF6MXcV.exe modified
14:36:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run firefox "C:\Users\user\AppData\Roaming\firefox.exe"

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
chongmei33.publicvm.com	ORDER_2110225_pdf.jar	Get hash	malicious	Browse	• 141.101.134.18
	Order_ Inquiry_Octorber_pdf.jar	Get hash	malicious	Browse	• 141.101.134.18
	mt103_usd78654_pdf.jar	Get hash	malicious	Browse	• 141.101.134.47
	ORDER_211099A_pdf.jar	Get hash	malicious	Browse	• 141.101.134.47
	spnxsdsnu.jar	Get hash	malicious	Browse	• 141.101.134.18
	ORDER-0021889.jar	Get hash	malicious	Browse	• 141.101.134.18
	spnxsdsnu.jar	Get hash	malicious	Browse	• 141.101.134.18
	ORDER-0021889.jar	Get hash	malicious	Browse	• 141.101.134.18
	SecuriteInfo.com.Heur.MSIL.Androm.1.13901.exe	Get hash	malicious	Browse	• 141.101.134.39
	01_extracted.jar	Get hash	malicious	Browse	• 172.94.109.53
	AVZ80SGiM1.exe	Get hash	malicious	Browse	• 141.101.134.44
	rz89FRwKvB.exe	Get hash	malicious	Browse	• 172.94.109.9
	6VYNUalwUt.exe	Get hash	malicious	Browse	• 46.243.221.18
	ORDER-6010.pdf.exe	Get hash	malicious	Browse	• 46.243.221.22
	ORDER-210067.xls.exe	Get hash	malicious	Browse	• 46.243.221.40
	ORDER-02188.exe	Get hash	malicious	Browse	• 46.243.217.11
	PO-21055-COPY.xls.jar	Get hash	malicious	Browse	• 46.243.217.36
	PO-21322.xlsm	Get hash	malicious	Browse	• 46.243.221.36
	PO-21789669S_pdf.jar	Get hash	malicious	Browse	• 46.243.221.30
	PO-21789669S_pdf.jar	Get hash	malicious	Browse	• 46.243.221.30

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NETZBETRIEB-GMBHDE	spnxsdsnu.jar	Get hash	malicious	Browse	• 141.101.134.18
	ORDER-0021889.jar	Get hash	malicious	Browse	• 141.101.134.18
	spnxsdsnu.jar	Get hash	malicious	Browse	• 141.101.134.18
	ORDER-0021889.jar	Get hash	malicious	Browse	• 141.101.134.18
	SecuriteInfo.com.Heur.MSIL.Androm.1.13901.exe	Get hash	malicious	Browse	• 141.101.134.51
	uCXiXf5LvT	Get hash	malicious	Browse	• 93.159.212.227
	dGSQxmfNFwvn.exe	Get hash	malicious	Browse	• 141.101.134.37
	AVZ80SGiM1.exe	Get hash	malicious	Browse	• 141.101.134.44
	JVB30EDCaR	Get hash	malicious	Browse	• 93.159.212.251
	http://https://rediree3.from-wv.com/black1/	Get hash	malicious	Browse	• 80.255.2.39
	http://195.138.255.24	Get hash	malicious	Browse	• 195.138.255.24
	B0B.exe	Get hash	malicious	Browse	• 81.95.5.133
	#U0413#U0430#U0437#U043f#U0440#U043e#U043c#U0431#U0430#U043d#U043a #U0437#U0430#U043a#U0430#U0437.js	Get hash	malicious	Browse	• 82.199.155.89
	100213865.doc.js	Get hash	malicious	Browse	• 92.43.107.180
	100213865.doc.js	Get hash	malicious	Browse	• 92.43.107.180
	24Faktura-2018_10_03_PDF.exe	Get hash	malicious	Browse	• 80.255.6.23
	http://https://puhavuz.cf/cgi-ssl/file-directory/access-secured/finder/microsoftonline365.com.auth/login.php?userid=samuel.tietjen@motiva.com	Get hash	malicious	Browse	• 195.138.255.18
	xv17XXqvDA.doc	Get hash	malicious	Browse	• 80.255.3.109

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2FXSF6MXcV.exe.log

Process:	C:\Users\user\Desktop\2FXSF6MXcV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	612
Entropy (8bit):	5.33730556823153

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2FXSF6MXcV.exe.log	
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21xzAbDLI4M0kvoDLI4MWuCOKbbDLI4MWuPJKiUrRZ9l0ZKhk:ML9E4Ks2vsXE4jE4KnKDE4KhK3VZ9pKe
MD5:	08A80BA6C9FA7AD518949631A37A08F9
SHA1:	27D59DD0D98BE6A7986BD690F9290451CAFD1536
SHA-256:	BDBB0129FD9D6760CB29D06B764A239A2E21DE7792CF0415211FBDF5551519FE
SHA-512:	CF00287F65F7D19C66F6AE2BEABAA9A442A5202F39E05B7E67BB56391212FDA0E06DB1F671A2A9CD52F3C12C230EAB7C0C6822A89CAAF5DBEDF14E9B84FA2C16
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe	
Process:	C:\Users\user\Desktop\2FXSF6MXcV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	544256
Entropy (8bit):	7.634719012543835
Encrypted:	false
SSDEEP:	12288:flGhdMhckf/KMU1oHh6ZL2tJ84K0AQZ+3GS4Wwt4q4W8wL:cAhceEshcqtJ84K0f+3gt4n
MD5:	E13B24CDA6737F13B2DC3F2C20D8823B
SHA1:	B58A2436A4BEFB5B7465153A72F64FD17531644C
SHA-256:	F8EE546F04FA175FA9A8B1F3DE8595BD0A4F6AEBFEED50A95C5E309D49063E1E
SHA-512:	C8FD34D209A8659638E349A86FC39F76A11EE0A7A74AFB4DB479D7C00A6442194A3E3FF9AAE41EFB6ACD065F2CF665342FD523AA19FE69CB95B0178F903B734C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....va..... .....@.. ..... .@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....L.....@..B.....H.....t4..H!.....U...R.....:....&(....8....*8....&8....8.....8....*s....(....t....:....&8....8....8....8.....8.....~....*.&~. .....*...~....*..0.....8y.....E....'...R...8"...* ....9{...&8.....Y.:z...&8....8.... ....~m...9....& ....8.....(....85....:....8....8....8.....:....8....&8....8.....8....8....(....8....8|..... ....~n...:G ...&8=....0.....9....&8.....E....B.....8=.....(....9:... ....~`

C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\2FXSF6MXcV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\firefox.exe	
Process:	C:\Users\user\AppData\Roaming\firefox.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	544256
Entropy (8bit):	7.634719012543835
Encrypted:	false
SSDEEP:	12288:flGhdMhckf/KMU1oHh6ZL2tJ84K0AQZ+3GS4Wwt4q4W8wL:cAhceEshcqtJ84K0f+3gt4n
MD5:	E13B24CDA6737F13B2DC3F2C20D8823B
SHA1:	B58A2436A4BEFB5B7465153A72F64FD17531644C

C:\Users\user\AppData\Local\Temp\firefox.exe	
SHA-256:	F8EE546F04FA175FA9A8B1F3DE8595BD0A4F6AEBFEED50A95C5E309D49063E1E
SHA-512:	C8FD34D209A8659638E349A86FC39F76A11EE0A7A74AFB4DB479D7C00A6442194A3E3FF9AAE41EFB6ACD065F2CF665342FD523AA19FE69CB95B0178F903B734C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....va..... .....@.. ..... .@.....K..... ....L.....@..B.....H.....t4..H!.....U...R.....:...&(....8....*8....&8....8.....8....*s....(....t....:....&8....8....8....8.....8.....~....*.&~. .....*...~....*..0.....8y.....E....'...R...8"...* ....9{...&8.....Y.:z...&8....8.... ....~m...9....& ....8.....(....85.....:....8....8....8.....:....8....&8....8.....8....8....(....8....8|..... ....~n...:G ...&8=....0.....9....&8.....E....B.....8=.....(....9:... ....~`

C:\Users\user\AppData\Local\Temp\firefox.exe:Zone.Identifier	
Process:	C:\Users\user\AppData\Roaming\firefox.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:1atn:Itn
MD5:	C0B4C5D70A426481C367FCD275C1E527
SHA1:	17E1FBDE70F34257DACDFAD013E5F763A57E443D
SHA-256:	0E9F810198356BE0880ADCAE0914A8714C09C71AA59F34F426D1AD9FF9B16B3F
SHA-512:	F9064E31C160D62F2648F1EE1F169B0BFCA159E117A4F0A36AEC841CF9D2909C4A1AE188C499573E3DD539C7DC49197DF1F74B35E6C2D30EA504C483C8BD35E
Malicious:	**true**
Reputation:	low
Preview:	.....H

C:\Users\user\AppData\Roaming\firefox.exe	
Process:	C:\Users\user\Desktop\2FXSF6MXcV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	544256
Entropy (8bit):	7.634719012543835
Encrypted:	false
SSDEEP:	12288:flGhdMhckf/KMU1oHh6ZL2tJ84K0AQZ+3GS4Wwt4q4W8wL:cAhceEshcqtJ84K0f+3gt4n
MD5:	E13B24CDA6737F13B2DC3F2C20D8823B
SHA1:	B58A2436A4BEFB5B7465153A72F64FD17531644C
SHA-256:	F8EE546F04FA175FA9A8B1F3DE8595BD0A4F6AEBFEED50A95C5E309D49063E1E
SHA-512:	C8FD34D209A8659638E349A86FC39F76A11EE0A7A74AFB4DB479D7C00A6442194A3E3FF9AAE41EFB6ACD065F2CF665342FD523AA19FE69CB95B0178F903B734C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%

C:\Users\user\AppData\Roaming\firefox.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....va..... .....@.. ..... .@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....L.....@..B.....H.....t4..H!.....U...R.....:...&(....8....*8....&8....8.....8....*s....(....t....:....&8....8....8....8.....8.....~....*.&~. .....*...~....*..0.....8y.....E....'...R...8"...* ....9{...&8.....Y.:z...&8....8.... ....~m...9....& ....8.....(....85....:....8....8....8.....:....8....&8....8.....8....8....(....8....8|..... ....~n...:G ...&8=....0.....9....&8.....E....B.....8=.....(....9:... ....~`

C:\Users\user\AppData\Roaming\firefox.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\2FXSF6MXcV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.634719012543835
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:	2FXSF6MXcV.exe
File size:	544256
MD5:	e13b24cda6737f13b2dc3f2c20d8823b
SHA1:	b58a2436a4befb5b7465153a72f64fd17531644c
SHA256:	f8ee546f04fa175fa9a8b1f3de8595bd0a4f6aebfeed50a95c5e309d49063e1e
SHA512:	c8fd34d209a8659638e349a86fc39f76a11ee0a7a74afb4db479d7c00a6442194a3e3ff9aae41efb6acd065f2cf665342fd523aa19fe69cb95b0178f903b734c
SSDEEP:	12288:flGhdMhckf/KMU1oHh6ZL2tJ84K0AQZ+3GS4Wwt4q4W8wL:cAhceEshcqtJ84K0f+3gt4n
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....va..... .....@.. .....@.....

File Icon

Icon Hash:	70f0d8d4d4d8f069

Static PE Info

General

Entrypoint:	0x46a8ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6176EE13 [Mon Oct 25 17:49:07 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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	0x688f4	0x68a00	False	0.988344254032	data	7.99260887475	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x1bfa4	0x1c000	False	0.217694963728	data	4.88488417465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 26, 2021 14:36:07.299653053 CEST	192.168.2.3	8.8.8.8	0x3c6d	Standard query (0)	chongmei33.publicvm.com	A (IP address)	IN (0x0001)
Oct 26, 2021 14:36:26.549268007 CEST	192.168.2.3	8.8.8.8	0x5d6	Standard query (0)	chongmei33.publicvm.com	A (IP address)	IN (0x0001)
Oct 26, 2021 14:36:43.356201887 CEST	192.168.2.3	8.8.8.8	0x3811	Standard query (0)	chongmei33.publicvm.com	A (IP address)	IN (0x0001)
Oct 26, 2021 14:37:00.459346056 CEST	192.168.2.3	8.8.8.8	0x43d2	Standard query (0)	chongmei33.publicvm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 14:36:07.420595884 CEST	8.8.8.8	192.168.2.3	0x3c6d	No error (0)	chongmei33 .publicvm.com		141.101.134.20	A (IP address)	IN (0x0001)
Oct 26, 2021 14:36:26.716905117 CEST	8.8.8.8	192.168.2.3	0x5d6	No error (0)	chongmei33 .publicvm.com		141.101.134.20	A (IP address)	IN (0x0001)
Oct 26, 2021 14:36:43.375072002 CEST	8.8.8.8	192.168.2.3	0x3811	No error (0)	chongmei33 .publicvm.com		141.101.134.20	A (IP address)	IN (0x0001)
Oct 26, 2021 14:37:00.477619886 CEST	8.8.8.8	192.168.2.3	0x43d2	No error (0)	chongmei33 .publicvm.com		141.101.134.20	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 2FXSF6MXcV.exe PID: 6132 Parent PID: 5332

General

Start time:	14:34:58
Start date:	26/10/2021
Path:	C:\Users\user\Desktop\2FXSF6MXcV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\2FXSF6MXcV.exe'
Imagebase:	0xce0000
File size:	544256 bytes
MD5 hash:	E13B24CDA6737F13B2DC3F2C20D8823B
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: 00000000.00000003.404881543.00000000043C7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.404881543.00000000043C7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.404881543.00000000043C7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.422619914.000000000437F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.422619914.000000000437F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.422619914.000000000437F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.416883288.00000000031A3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.416883288.00000000031A3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.417608309.0000000004101000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.417608309.0000000004101000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.417608309.0000000004101000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: svchost.exe PID: 4936 Parent PID: 572

General

Start time:	14:35:25
Start date:	26/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: 2FXSF6MXcV.exe PID: 4936 Parent PID: 6132

General

Start time:	14:35:57
Start date:	26/10/2021
Path:	C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2FXSF6MXcV.exe
Imagebase:	0xff0000
File size:	544256 bytes
MD5 hash:	E13B24CDA6737F13B2DC3F2C20D8823B
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: 00000013.00000000.410602716.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.410602716.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.410602716.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.411789598.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.411789598.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.411789598.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.556312949.00000000065E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.556312949.00000000065E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.556312949.00000000065E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.411248412.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.411248412.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.411248412.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.412380595.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.412380595.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.412380595.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.554569940.00000000043B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.554569940.00000000043B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.549310054.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.549310054.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.549310054.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.556187820.0000000006530000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.556187820.0000000006530000.00000004.00020000.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 33%, ReversingLabs
Reputation:	low

File Activities | Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: firefox.exe PID: 5536 Parent PID: 3352

General

Start time:	14:36:05
Start date:	26/10/2021
Path:	C:\Users\user\AppData\Roaming\firefox.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\firefox.exe'
Imagebase:	0xdd0000
File size:	544256 bytes
MD5 hash:	E13B24CDA6737F13B2DC3F2C20D8823B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 33%, ReversingLabs
Reputation:	low

File Activities | Show Windows behavior

File Read

Analysis Process: firefox.exe PID: 6312 Parent PID: 3352

General

Start time:	14:36:13
Start date:	26/10/2021
Path:	C:\Users\user\AppData\Roaming\firefox.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\firefox.exe'
Imagebase:	0xd80000
File size:	544256 bytes
MD5 hash:	E13B24CDA6737F13B2DC3F2C20D8823B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities | Show Windows behavior

File Read

Disassembly

Code Analysis