ID: 342477
Sample Name: PO#4018-308875.exe
Cookbook: default.jbs
Time: 07:18:42
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report PO#4018-308875.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Compliance: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 17

Data Directories 18
Sections 18
Resources 19
Imports 19
Version Infos 19
Possible Origin 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 20
UDP Packets 21
DNS Queries 23
DNS Answers 23
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: PO#4018-308875.exe PID: 5652 Parent PID: 5668 24
General 24
File Activities 25
File Created 25
File Written 25
File Read 26
Analysis Process: cmd.exe PID: 4564 Parent PID: 5652 27
General 27
File Activities 27
Analysis Process: conhost.exe PID: 4496 Parent PID: 4564 27
General 27
Analysis Process: reg.exe PID: 2764 Parent PID: 4564 27
General 28
File Activities 28
Registry Activities 28
Key Value Created 28
Analysis Process: hjfufkimd.exe PID: 4408 Parent PID: 5652 28
General 28
File Activities 28
File Created 28
File Read 29
Analysis Process: InstallUtil.exe PID: 7088 Parent PID: 4408 29
General 29
File Activities 30
File Created 30
File Written 30
File Read 31
Disassembly 31
Code Analysis 31

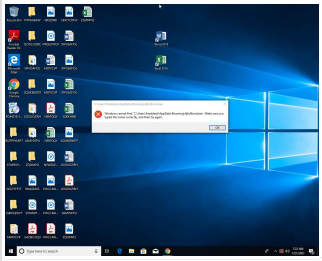
Analysis Report PO#4018-308875.exe

Overview

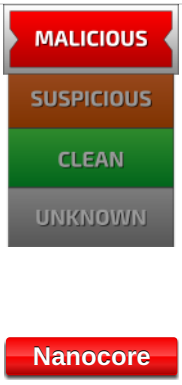
General Information

Sample Name:	PO#4018-308875.exe
Analysis ID:	342477
MD5:	26b17b353c8950..
SHA1:	c5f2e80f53a312b..
SHA256:	43bdef53f8ff0d26..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



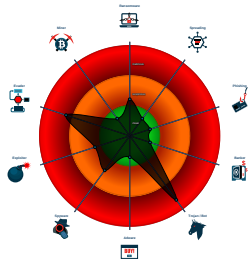
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains very larg…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Uses dynamic DNS services
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- PO#4018-308875.exe (PID: 5652 cmdline: 'C:\Users\user\Desktop\PO#4018-308875.exe' MD5: 26B17B353C8950CA0A55E1EA21678D9E)
  - cmd.exe (PID: 4564 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'erwtvsfvc' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hjfufkimd.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 2764 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'erwtvsfvc' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hjfufkimd.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - hjfufkimd.exe (PID: 4408 cmdline: 'C:\Users\user\AppData\Roaming\hjfufkimd.exe' MD5: 26B17B353C8950CA0A55E1EA21678D9E)
    - InstallUtil.exe (PID: 7088 cmdline: C:\Users\user~1\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.162.88.26",
    "185.162.88.26:2091"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000014.00000002.632887895.000000000493 5000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xdb8ef:$x1: NanoCore.ClientPluginHost • 0x10e4bf:$x1: NanoCore.ClientPluginHost • 0x14107f:$x1: NanoCore.ClientPluginHost • 0xdb92c:$x2: IClientNetworkHost • 0x10e4fc:$x2: IClientNetworkHost • 0x1410bc:$x2: IClientNetworkHost • 0xdf45f:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x11202f:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x144bef:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000014.00000002.632887895.000000000493 5000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000014.00000002.632887895.000000000493 5000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xdb657:$a: NanoCore • 0xdb667:$a: NanoCore • 0xdb89b:$a: NanoCore • 0xdb8af:$a: NanoCore • 0xdb8ef:$a: NanoCore • 0x10e227:$a: NanoCore • 0x10e237:$a: NanoCore • 0x10e46b:$a: NanoCore • 0x10e47f:$a: NanoCore • 0x10e4bf:$a: NanoCore • 0x140de7:$a: NanoCore • 0x140df7:$a: NanoCore • 0x14102b:$a: NanoCore • 0x14103f:$a: NanoCore • 0x14107f:$a: NanoCore • 0xdb6b6:$b: ClientPlugin • 0xdb8b8:$b: ClientPlugin • 0xdb8f8:$b: ClientPlugin • 0x10e286:$b: ClientPlugin • 0x10e488:$b: ClientPlugin • 0x10e4c8:$b: ClientPlugin
0000001A.00000002.632805982.000000000562 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
0000001A.00000002.632805982.000000000562 0000.00000004.00000001.sdmp	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 23 entries				

Unpacked PEs

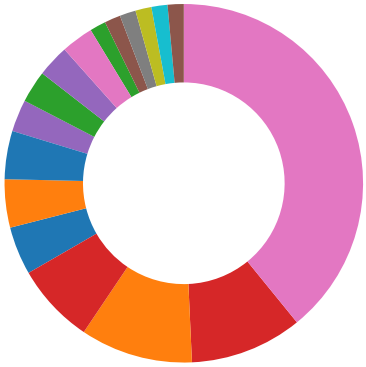
Source	Rule	Description	Author	Strings
26.2.InstallUtil.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
26.2.InstallUtil.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
26.2.InstallUtil.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
26.2.InstallUtil.exe.400000.0.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:$j: #=q
26.2.InstallUtil.exe.5620000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

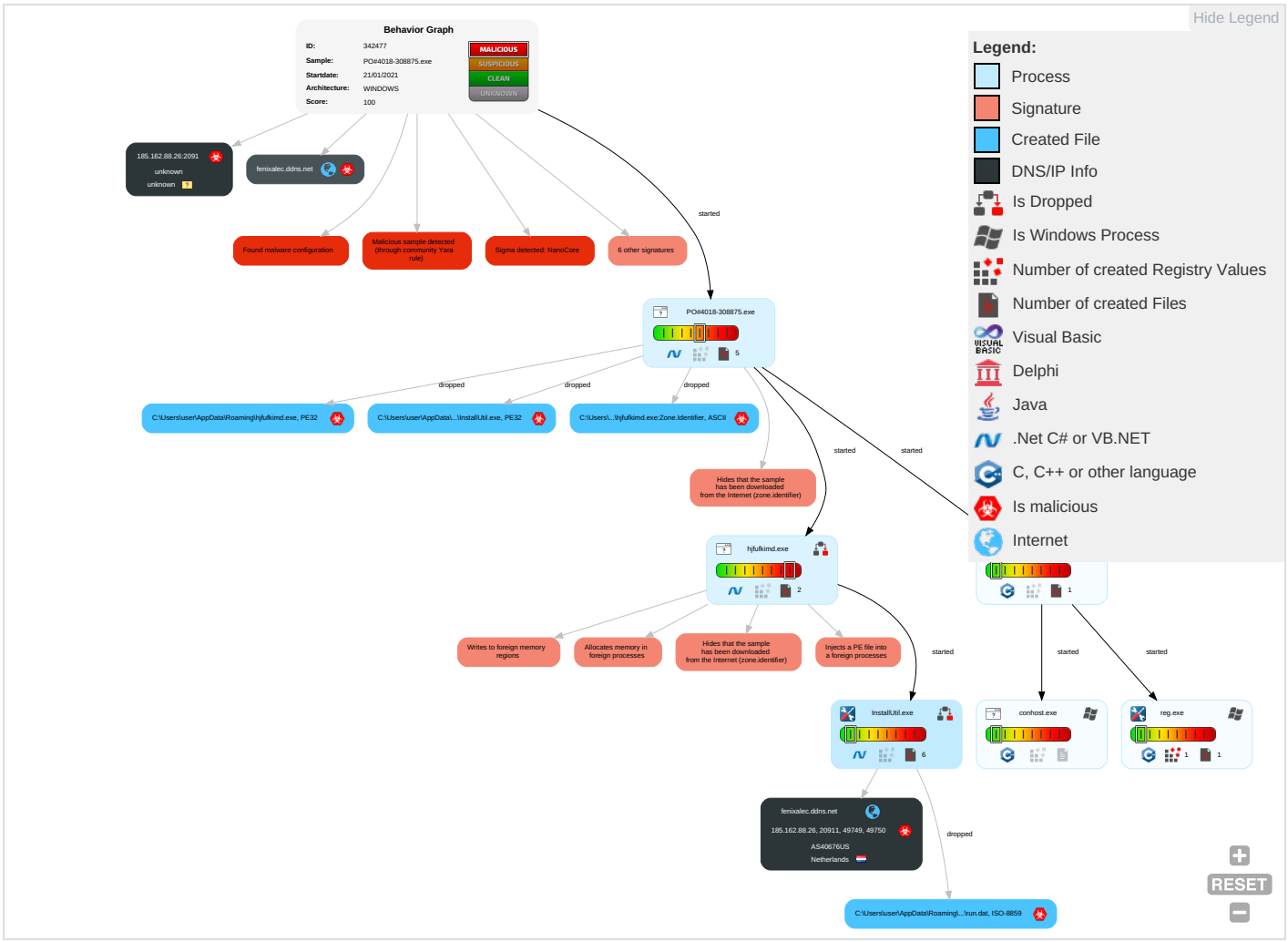
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation	Valid Accounts 1	Valid Accounts 1	Masquerading 1	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-S Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Modify Registry 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remot Softwa
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applic Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Applic Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Disable or Modify Tools 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Software Packing 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

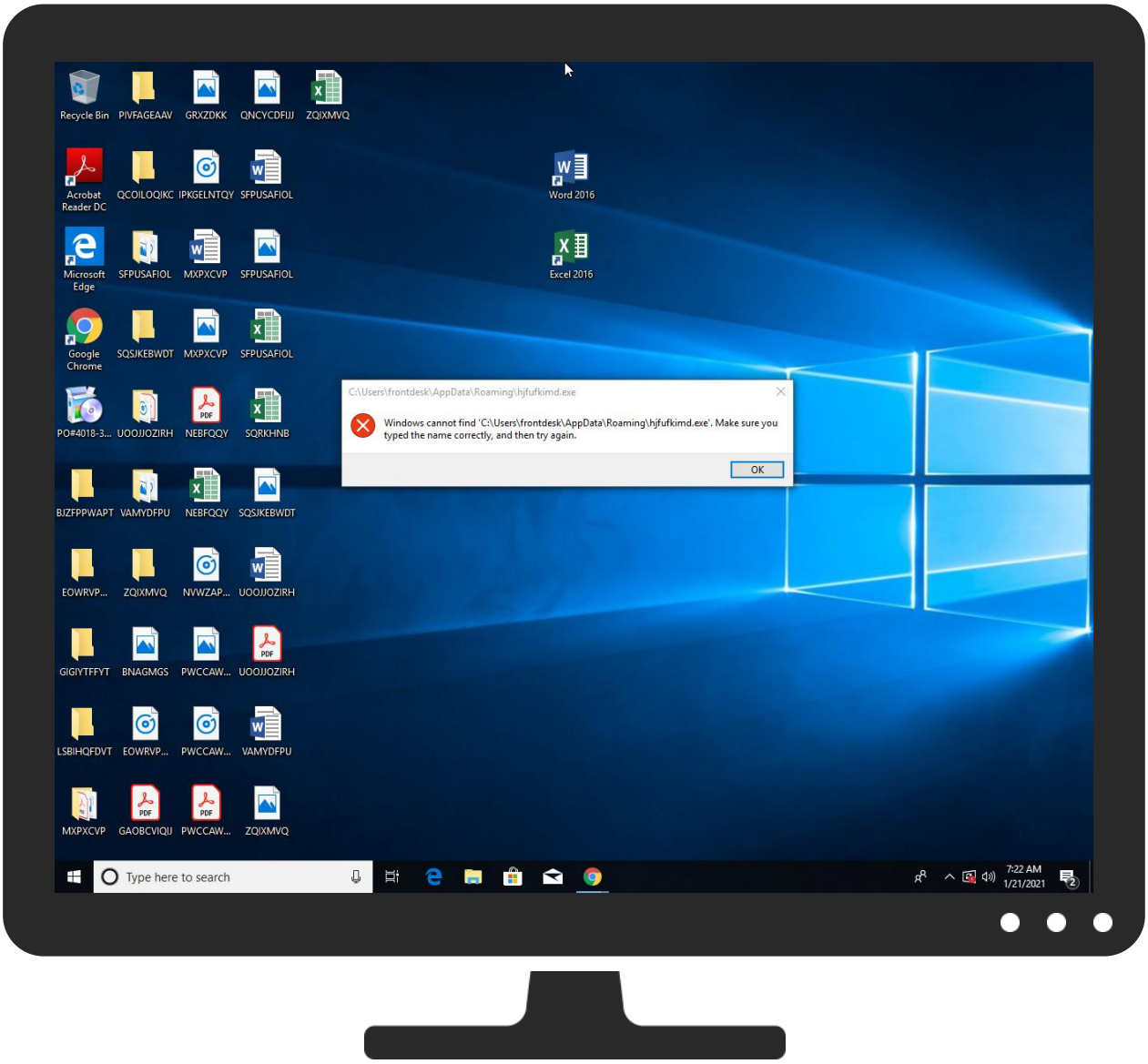
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
26.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
26.2.InstallUtil.exe.5f00000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
fenixalec.ddns.net	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ns.ado/Ident	0%	Avira URL Cloud	safe	
http://iptc.tc4xmp	0%	Avira URL Cloud	safe	

Domains and IPs

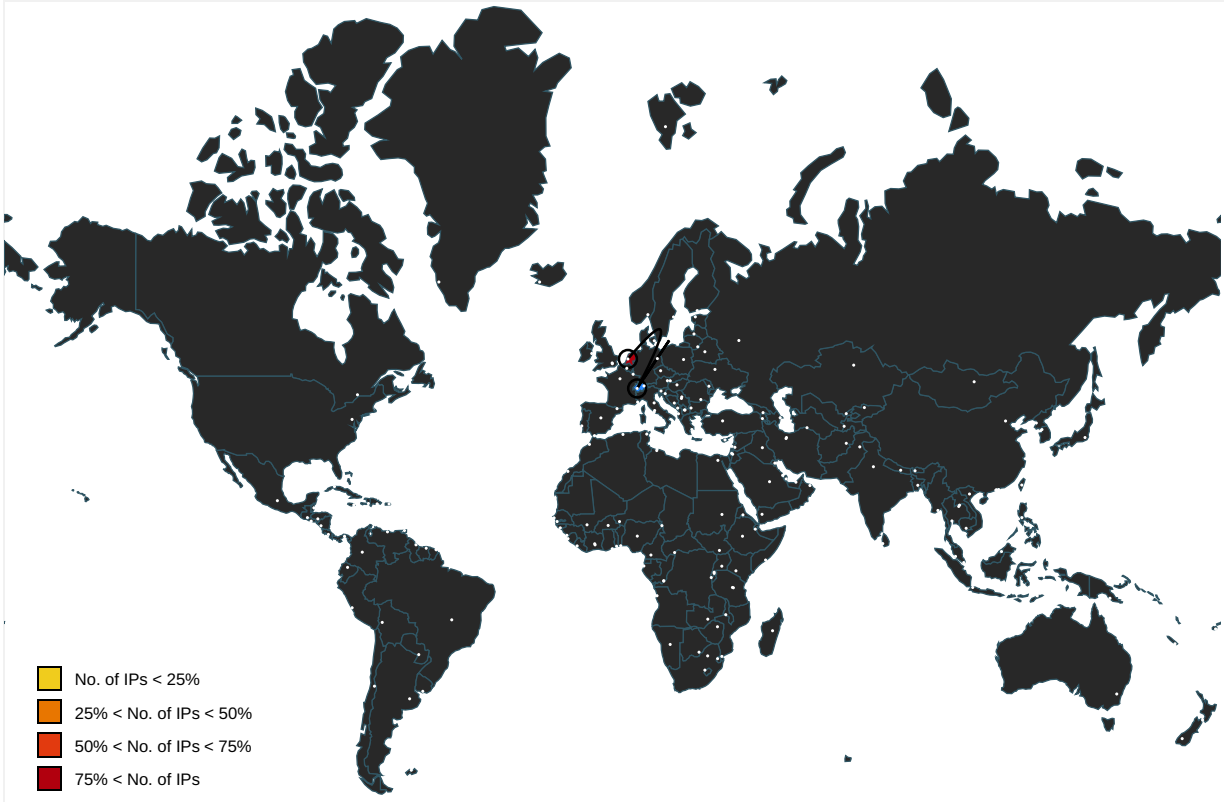
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fenixalec.ddns.net	185.162.88.26	true	true	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.ado/Ident	PO#4018-308875.exe, 00000000.0000000 3.337497700.00000000015A9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.tc4xmp	hjfufkimd.exe, 00000014.00000002.626448750.00000000016C9000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.162.88.26:2091	unknown	unknown	?	unknown	unknown	true
185.162.88.26	unknown	Netherlands		40676	AS40676US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond

Analysis ID:	342477
Start date:	21.01.2021
Start time:	07:18:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#4018-308875.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:	31
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@10/5@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2% (good quality ratio 1.9%) • Quality average: 49.5% • Quality standard deviation: 23.9%
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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.42.151.234, 2.20.84.85, 51.11.168.160, 92.122.213.194, 92.122.213.247, 51.103.5.186, 205.185.216.10, 205.185.216.42, 52.155.217.156, 20.54.26.129, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:19:43	API Interceptor	188x Sleep call for process: PO#4018-308875.exe modified
07:19:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run erwtvsfvc C:\Users\user\AppData\Roaming\hjfufkimd.exe
07:19:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run erwtvsfvc C:\Users\user\AppData\Roaming\hjfufkimd.exe
07:20:30	API Interceptor	204x Sleep call for process: hjfufkimd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.162.88.26	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fenixalec.ddns.net	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS40676US	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Ulma9B5jo1.exe	Get hash	malicious	Browse	• 104.149.57.92
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Request for Quotation.exe	Get hash	malicious	Browse	• 45.34.249.53
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	t1XJOlYvhExZyrm.exe	Get hash	malicious	Browse	• 104.225.208.15
	SWIFT_COPY00993Payment_advic4555pdf.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 104.149.57.92
	SWIFT-COPY Payment advice3243343.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	NPD76122.exe	Get hash	malicious	Browse	• 104.217.23 1.247
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	d2mISAbTQN.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	n41pVXkYCe.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	53McmgaUJP.exe	Get hash	malicious	Browse	• 104.217.23 1.248

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	IMG_57880.pdf.exe	Get hash	malicious	Browse	
	PO 67542 PDF.exe	Get hash	malicious	Browse	
	Mi9eI6wu1p.exe	Get hash	malicious	Browse	
	OJ4zX7G77Y.exe	Get hash	malicious	Browse	
	IMG_50781.pdf.exe	Get hash	malicious	Browse	
	IMG_25579.pdf.exe	Get hash	malicious	Browse	
	IMG_40317.pdf.exe	Get hash	malicious	Browse	
	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.8504.exe	Get hash	malicious	Browse	
	IMG_80137.pdf.exe	Get hash	malicious	Browse	
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2GNCGUZ6JU.exe	Get hash	malicious	Browse	
	IMG_53771.pdf.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.fb5363e0cae04979.exe	Get hash	malicious	Browse	
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	
	74725794.exe	Get hash	malicious	Browse	
	74725794.exe	Get hash	malicious	Browse	
	IMG_53091.pdf.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.exe.log	
Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895E ABB
Malicious:	false
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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe

Joe Sandbox View:	• Filename: IMG_57880.pdf.exe, Detection: malicious, Browse • Filename: PO 67542 PDF.exe, Detection: malicious, Browse • Filename: Mi9el6wu1p.exe, Detection: malicious, Browse • Filename: OJ4zX7G77Y.exe, Detection: malicious, Browse • Filename: IMG_50781.pdf.exe, Detection: malicious, Browse • Filename: IMG_25579.pdf.exe, Detection: malicious, Browse • Filename: IMG_40317.pdf.exe, Detection: malicious, Browse • Filename: PO#4018-308875.pdf.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.8504.exe, Detection: malicious, Browse • Filename: IMG_80137.pdf.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: MEDUSI492126.pdf.exe, Detection: malicious, Browse • Filename: 2GNCGUZ6JU.exe, Detection: malicious, Browse • Filename: IMG_53771.pdf.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.fb5363e0cae04979.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: silkOrder00110.pdf.exe, Detection: malicious, Browse • Filename: 74725794.exe, Detection: malicious, Browse • Filename: 74725794.exe, Detection: malicious, Browse • Filename: IMG_53091.pdf.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

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

Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:R:R
MD5:	2F1BE7A93FA3932139F44045B7093C9D
SHA1:	3BD21ABDB1D8DF0DB4FB6584AE3E957B4BC09F36
SHA-256:	FC8D923CBCB211095CFD934D23AA52DD05FDD272545BD4CB488D15A186BAA53D
SHA-512:	530C64B9C169A53F0721317D1D7AE338C75EED8A6925D512172198875DD3DFF63CE9DB5FECB29685B773E29589DF3AB2FE44D2D035A7539EBFE67CA3DA0680A 4
Malicious:	**true**
Reputation:	low
Preview:	..&- ..H

C:\Users\user\AppData\Roaming\hjfufkimd.exe

Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	716800
Entropy (8bit):	5.544271789349581
Encrypted:	false
SSDEEP:	12288:jJ050jwcEc6t4HpTkJ23d9ZSn9Vt6DuUx:ji08cEc6t4HpAlZSnb
MD5:	26B17B353C8950CA0A55E1EA21678D9E
SHA1:	C5F2E80F53A312BD1B8DD3BBA438AF27A4BA44E3
SHA-256:	43BDEF53F8FF0D262C2086A46C66D76F8C5E2B9DF085959C70A5A3C679474767
SHA-512:	B90A04A218AE54201A4AB25848C91DC197C829C90BEB4DE4B8CC5F9F54928A962151129796181B9DBF48DA1BE6BB7294F878E3BDF020373B9DF2C8A759E8BE2 3
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m..G.....~...p.....^.... .....@.. .....@ .....`.....S.....I..... ..... ..... ..H.....text...d|... ...~..... ..`.rsrc....I.....n.....@..@.rel oc..... .....@..B.....@.....H.....`..0;.....<....*...6.....w.....%.v..y.....d..:....m....Q.....4..W.....F..s.n..y!sv.g..+'....=6.S...^..g.L..z... G\|;g\|@.R....Nj..2hLX.^s....Z.[G.4.....c..4.b..../.z+..X.%.....K....[...D.?Iq.#."..=...3.-..k.P...^..;.+...6..j..ig.....-...E1.*Z.0.e...4.....J.G..C.C...1..h...I..N>.U]}..T6jZ...Dq.yDY.y. .8.....M.2.Jia&..C\...q...q..t...u$.]N....V.\....U.V....R.._.}N.a....c....h}.J/N..J.i..-`j.SL.....(6.._....

C:\Users\user\AppData\Roaming\hjfufkimd.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\hjfufkimd.exe:Zone.Identifier	
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.544271789349581
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO#4018-308875.exe
File size:	716800
MD5:	26b17b353c8950ca0a55e1ea21678d9e
SHA1:	c5f2e80f53a312bd1b8dd3bba438af27a4ba44e3
SHA256:	43bdef53f8ff0d262c2086a46c66d76f8c5e2b9df085959c70a5a3c679474767
SHA512:	b90a04a218ae54201a4ab25848c91dc197c829c90beb4de4b8cc5f9f54928a962151129796181b9dbf48da1be6bb7294f878e3bdf020373b9df2c8a759e8be23
SSDEEP:	12288:jJ050jwcEc6t4HpTkJ23d9ZSn9Vt6DuUx:ji08cEc6t4HpAIZSnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m..G.....~...p.....^.... .....@.. .....@.....`.....

File Icon

Icon Hash:	6862eee6b292c66e

Static PE Info

General

Entrypoint:	0x4a9c5e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x471CEA6D [Mon Oct 22 18:22:37 2007 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa9c08	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0x6c0e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa7c64	0xa7e00	False	0.528291953649	data	5.50950484926	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x6c0e	0x6e00	False	0.521803977273	data	5.77182057685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xaa2c4	0x668	data		
RT_ICON	0xaa92c	0x2e8	data		
RT_ICON	0xaac14	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0xaad3c	0xea8	data		
RT_ICON	0xabbe4	0x8a8	data		
RT_ICON	0xac48c	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xac9f4	0x25a8	data		
RT_ICON	0xaef9c	0x10a8	data		
RT_ICON	0xb0044	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xb04ac	0x84	data		
RT_VERSION	0xb0530	0x4f4	data	English	United States
RT_MANIFEST	0xb0a24	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	(c) Nota Inc. All rights reserved.
FileVersion	4.1.4.0
CompanyName	Nota Inc.
Comments	This installation was built with Inno Setup.
ProductName	Gyazo
ProductVersion	4.1.4.0
FileDescription	Gyazo Setup
Translation	0x0000 0x04b0

Possible Origin

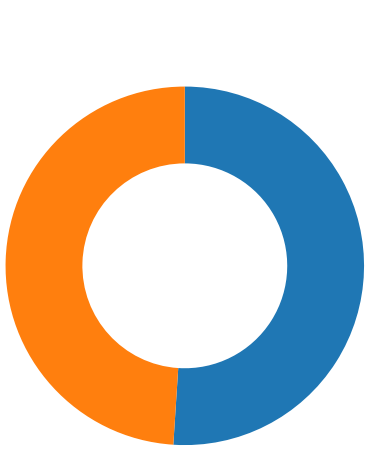
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 98

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:21:10.194595098 CET	49749	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:10.245362997 CET	20911	49749	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:10.750391960 CET	49749	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:10.800987005 CET	20911	49749	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:11.312966108 CET	49749	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:11.363570929 CET	20911	49749	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:15.517932892 CET	49750	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:15.568631887 CET	20911	49750	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:16.079057932 CET	49750	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:16.129749060 CET	20911	49750	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:16.641479969 CET	49750	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:16.692219973 CET	20911	49750	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:20.705828905 CET	49751	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:20.756248951 CET	20911	49751	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:21.267081976 CET	49751	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:21.317872047 CET	20911	49751	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:21.829600096 CET	49751	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:21.880040884 CET	20911	49751	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:26.059458971 CET	49753	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:26.110008955 CET	20911	49753	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:26.611205101 CET	49753	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:26.661964893 CET	20911	49753	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:27.174010992 CET	49753	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:27.224834919 CET	20911	49753	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:31.299650908 CET	49755	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:31.350349903 CET	20911	49755	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:31.861526012 CET	49755	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:31.913264036 CET	20911	49755	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:32.424514055 CET	49755	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:32.475508928 CET	20911	49755	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:36.555077076 CET	49756	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:36.605745077 CET	20911	49756	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:37.112006903 CET	49756	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:37.162477016 CET	20911	49756	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:37.674544096 CET	49756	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:37.725790977 CET	20911	49756	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:41.746510983 CET	49757	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:41.797168016 CET	20911	49757	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:42.299890041 CET	49757	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:42.350419998 CET	20911	49757	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:42.862423897 CET	49757	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:42.913009882 CET	20911	49757	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:46.928580999 CET	49758	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:46.980833054 CET	20911	49758	185.162.88.26	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:21:47.487807035 CET	49758	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:47.538381100 CET	20911	49758	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:48.050369978 CET	49758	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:48.101048946 CET	20911	49758	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:52.114620924 CET	49759	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:52.165218115 CET	20911	49759	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:52.675843954 CET	49759	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:52.726166010 CET	20911	49759	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:53.238327026 CET	49759	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:53.288965940 CET	20911	49759	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:57.469202995 CET	49760	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:57.520087004 CET	20911	49760	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:58.035609961 CET	49760	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:58.086205959 CET	20911	49760	185.162.88.26	192.168.2.7
Jan 21, 2021 07:21:58.598628998 CET	49760	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:21:58.649328947 CET	20911	49760	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:02.790209055 CET	49761	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:02.840651989 CET	20911	49761	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:03.350677967 CET	49761	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:03.401880980 CET	20911	49761	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:03.910955906 CET	49761	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:03.961889982 CET	20911	49761	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:09.391566992 CET	49762	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:09.442047119 CET	20911	49762	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:09.952791929 CET	49762	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:10.004659891 CET	20911	49762	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:10.506259918 CET	49762	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:10.556945086 CET	20911	49762	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:14.601311922 CET	49763	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:14.652283907 CET	20911	49763	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:15.162935019 CET	49763	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:15.215492964 CET	20911	49763	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:15.725584984 CET	49763	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:15.777245045 CET	20911	49763	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:19.805321932 CET	49764	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:19.856096029 CET	20911	49764	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:20.366501093 CET	49764	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:20.417002916 CET	20911	49764	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:20.928977966 CET	49764	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:20.979587078 CET	20911	49764	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:25.120189905 CET	49765	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:25.170635939 CET	20911	49765	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:25.679419041 CET	49765	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:25.730566978 CET	20911	49765	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:26.241952896 CET	49765	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:26.292938948 CET	20911	49765	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:30.421901941 CET	49766	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:30.472906113 CET	20911	49766	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:30.976934910 CET	49766	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:31.027550936 CET	20911	49766	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:31.539257050 CET	49766	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:31.589936972 CET	20911	49766	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:35.667542934 CET	49767	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:35.718305111 CET	20911	49767	185.162.88.26	192.168.2.7
Jan 21, 2021 07:22:36.227289915 CET	49767	20911	192.168.2.7	185.162.88.26
Jan 21, 2021 07:22:36.277928114 CET	20911	49767	185.162.88.26	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:19:39.187886953 CET	55411	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:39.244185925 CET	53	55411	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:40.364118099 CET	63668	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:40.414766073 CET	53	63668	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:19:41.766908884 CET	54640	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:41.817589045 CET	53	54640	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:42.781416893 CET	58739	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:42.829230070 CET	53	58739	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:44.003678083 CET	60338	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:44.054332018 CET	53	60338	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:44.998965025 CET	58717	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:45.058206081 CET	53	58717	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:46.099541903 CET	59762	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:46.147551060 CET	53	59762	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:47.129146099 CET	54329	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:47.176958084 CET	53	54329	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:48.157058001 CET	58052	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:48.207770109 CET	53	58052	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:49.116137028 CET	54008	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:49.174880028 CET	53	54008	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:49.974899054 CET	59451	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:50.031143904 CET	53	59451	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:50.726120949 CET	52914	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:50.782291889 CET	53	52914	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:51.991139889 CET	64569	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:52.041958094 CET	53	64569	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:54.407627106 CET	52816	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:54.466856003 CET	53	52816	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:55.777554035 CET	50781	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:55.825472116 CET	53	50781	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:56.764731884 CET	54230	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:56.820934057 CET	53	54230	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:58.272994041 CET	54911	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:58.324692011 CET	53	54911	8.8.8.8	192.168.2.7
Jan 21, 2021 07:19:59.522815943 CET	49958	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:19:59.581321001 CET	53	49958	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:01.119352102 CET	50860	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:01.167102098 CET	53	50860	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:02.199868917 CET	50452	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:02.250752926 CET	53	50452	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:02.385554075 CET	59730	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:02.436297894 CET	53	59730	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:07.982062101 CET	59310	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:08.038496971 CET	53	59310	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:18.294717073 CET	51919	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:18.345320940 CET	53	51919	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:18.652225971 CET	64296	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:18.703476906 CET	53	64296	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:23.751013041 CET	56680	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:23.807271004 CET	53	56680	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:29.860162020 CET	58820	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:29.919303894 CET	53	58820	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:30.506624937 CET	60983	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:30.563065052 CET	53	60983	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:31.142412901 CET	49247	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:31.198556900 CET	53	49247	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:31.685444117 CET	52286	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:31.742531061 CET	53	52286	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:32.250085115 CET	56064	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:32.309338093 CET	53	56064	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:32.971565962 CET	63744	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:33.019469976 CET	53	63744	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:33.227957010 CET	61457	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:33.295059919 CET	53	61457	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:33.645874977 CET	58367	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:33.702230930 CET	53	58367	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:34.865190983 CET	60599	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:34.922327042 CET	53	60599	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:20:35.781820059 CET	59571	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:35.829627991 CET	53	59571	8.8.8.8	192.168.2.7
Jan 21, 2021 07:20:36.496061087 CET	52689	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:20:36.552227020 CET	53	52689	8.8.8.8	192.168.2.7
Jan 21, 2021 07:21:08.226511002 CET	50290	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:21:08.275254965 CET	53	50290	8.8.8.8	192.168.2.7
Jan 21, 2021 07:21:24.251454115 CET	60427	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:21:24.307600975 CET	53	60427	8.8.8.8	192.168.2.7
Jan 21, 2021 07:21:25.996978045 CET	56209	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:21:26.057513952 CET	53	56209	8.8.8.8	192.168.2.7
Jan 21, 2021 07:21:27.343066931 CET	59582	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:21:27.390883923 CET	53	59582	8.8.8.8	192.168.2.7
Jan 21, 2021 07:21:31.240375042 CET	60949	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:21:31.298129082 CET	53	60949	8.8.8.8	192.168.2.7
Jan 21, 2021 07:21:36.494344950 CET	58542	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:21:36.553634882 CET	53	58542	8.8.8.8	192.168.2.7
Jan 21, 2021 07:21:57.401041031 CET	59179	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:21:57.457227945 CET	53	59179	8.8.8.8	192.168.2.7
Jan 21, 2021 07:22:02.728920937 CET	60927	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:22:02.788012981 CET	53	60927	8.8.8.8	192.168.2.7
Jan 21, 2021 07:22:09.289910078 CET	57854	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:22:09.349340916 CET	53	57854	8.8.8.8	192.168.2.7
Jan 21, 2021 07:22:30.361867905 CET	62026	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:22:30.419929981 CET	53	62026	8.8.8.8	192.168.2.7
Jan 21, 2021 07:22:35.605401039 CET	59453	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:22:35.663017988 CET	53	59453	8.8.8.8	192.168.2.7
Jan 21, 2021 07:22:40.853759050 CET	62468	53	192.168.2.7	8.8.8.8
Jan 21, 2021 07:22:40.910154104 CET	53	62468	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2021 07:21:25.996978045 CET	192.168.2.7	8.8.8.8	0x34f5	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:21:31.240375042 CET	192.168.2.7	8.8.8.8	0x4116	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:21:36.494344950 CET	192.168.2.7	8.8.8.8	0x2199	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:21:57.401041031 CET	192.168.2.7	8.8.8.8	0x8b50	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:02.728920937 CET	192.168.2.7	8.8.8.8	0x6ffa	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:09.289910078 CET	192.168.2.7	8.8.8.8	0x8ace	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:30.361867905 CET	192.168.2.7	8.8.8.8	0xb7d8	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:35.605401039 CET	192.168.2.7	8.8.8.8	0xdeab	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:40.853759050 CET	192.168.2.7	8.8.8.8	0x60d	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

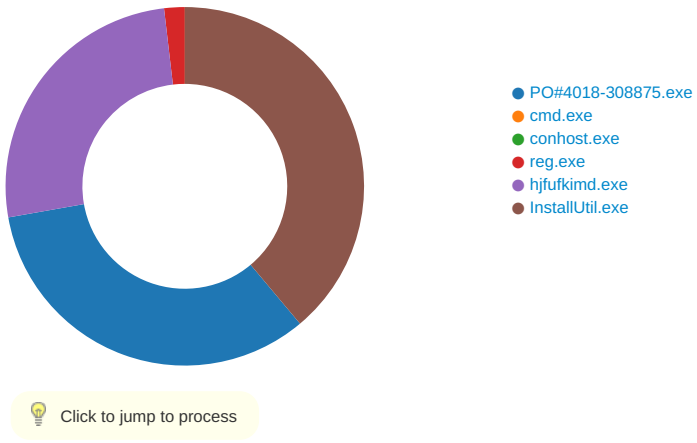
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 07:21:26.057513952 CET	8.8.8.8	192.168.2.7	0x34f5	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:21:31.298129082 CET	8.8.8.8	192.168.2.7	0x4116	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:21:36.553634882 CET	8.8.8.8	192.168.2.7	0x2199	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:21:57.457227945 CET	8.8.8.8	192.168.2.7	0x8b50	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:02.788012981 CET	8.8.8.8	192.168.2.7	0x6ffa	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 07:22:09.349340916 CET	8.8.8.8	192.168.2.7	0x8ace	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:30.419929981 CET	8.8.8.8	192.168.2.7	0xb7d8	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:35.663017988 CET	8.8.8.8	192.168.2.7	0xdeab	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:22:40.910154104 CET	8.8.8.8	192.168.2.7	0x60d	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO#4018-308875.exe PID: 5652 Parent PID: 5668

General

Start time:	07:19:36
Start date:	21/01/2021
Path:	C:\Users\user\Desktop\PO#4018-308875.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO#4018-308875.exe'
Imagebase:	0x9f0000
File size:	716800 bytes
MD5 hash:	26B17B353C8950CA0A55E1EA21678D9E
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: 00000000.00000002.339312543.00000000047A4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.339312543.00000000047A4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.339312543.00000000047A4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\InstallUtil.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	78CE9DB	CopyFileExW
C:\Users\user\AppData\Roaming\hjfufkimd.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	78CE9DB	CopyFileExW
C:\Users\user\AppData\Roaming\hjfufkimd.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	78CE9DB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0	41064	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 07 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 86 72 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....Z.Z..... ....0..T.....r... .....@.. ....`.....	success or wait	1	78CE9DB	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hjfufkimd.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6d ea 1c 47 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 7e 0a 00 00 70 00 00 00 00 00 00 5e 9c 0a 00 00 20 00 00 00 a0 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0b 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...m..G.......... ....~...p......^.... ....@.. ....@ ....`................	success or wait	3	78CE9DB	CopyFileExW
C:\Users\user\AppData\Roaming\hjfufkimd.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	78CE9DB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.exe.log	unknown	1451	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"Win RT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, Pub licKeyToken=b77a5c5619 34e089", "C:\Windows\assembly\Nat iveIma ges_v4.0.30319_32\Syste m\4f0a7 eefa3cd3e0ba98b5ebddbb c72e6\Sy stem.ni.dll",0..3,"Presentati onCore, Version=	success or wait	1	6D8EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D5103DE	ReadFile

Analysis Process: cmd.exe PID: 4564 Parent PID: 5652

General

Start time:	07:19:41
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'erwtvsfvc' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hjfufkimd.exe'
Imagebase:	0x1310000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4496 Parent PID: 4564

General

Start time:	07:19:41
Start date:	21/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 2764 Parent PID: 4564

General

Start time:	07:19:42
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'erwtvsfvc' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hjfufkimd.exe'
Imagebase:	0xd00000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	erwtvsfvc	unicode	C:\Users\user\AppData\Roaming\hjfufkimd.exe	success or wait	1	D05A1D	RegSetValueExW

Analysis Process: hjfufkimd.exe PID: 4408 Parent PID: 5652

General

Start time:	07:20:23
Start date:	21/01/2021
Path:	C:\Users\user\AppData\Roaming\hjfufkimd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\hjfufkimd.exe'
Imagebase:	0xb70000
File size:	716800 bytes
MD5 hash:	26B17B353C8950CA0A55E1EA21678D9E
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: 00000014.00000002.632887895.0000000004935000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.632887895.0000000004935000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.632887895.0000000004935000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.633244626.0000000004ACB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.633244626.0000000004ACB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.633244626.0000000004ACB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5B5705	unknown

Analysis Process: InstallUtil.exe PID: 7088 Parent PID: 4408

General

Start time:	07:21:01
Start date:	21/01/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x9b0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 0000001A.00000002.632805982.0000000005620000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000001A.00000002.632805982.0000000005620000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000002.633000163.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000001A.00000002.633000163.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.633000163.0000000005F00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000002.624554615.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.624554615.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.624554615.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.630562500.0000000003E99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.630562500.0000000003E99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5DCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C42BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C421E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C42BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C42BEFF	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	b5 a0 26 2d 20 be d8 48	..&- ..H	success or wait	1	6C421B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C421B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C421B4F	ReadFile
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	4096	success or wait	1	6D59D72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	512	success or wait	1	6D59D72F	unknown

Disassembly

Code Analysis