ID: 343937
Sample Name: PO#4018-308875.pdf.exe
Cookbook: default.jbs
Time: 19:20:18
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

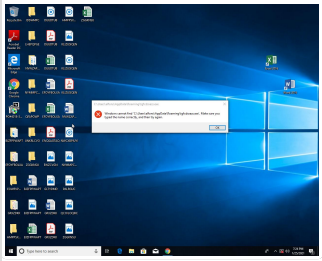
Analysis Report PO#4018-308875.pdf.exe

Overview

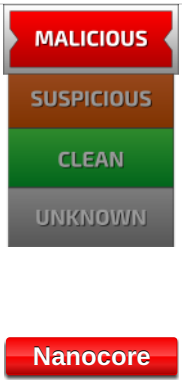
General Information

Sample Name:	PO#4018-308875.pdf.exe
Analysis ID:	343937
MD5:	ea28f2d01808072.
SHA1:	771ff981d42d6c7..
SHA256:	618d343a6d7f54a.
Tags:	exe NanoCore

Most interesting Screenshot:



Detection



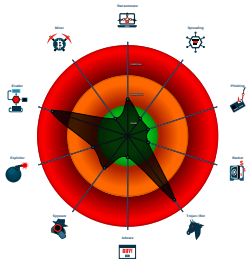
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- 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 …

Classification



Startup

- **System is w10x64**
- PO#4018-308875.pdf.exe (PID: 6520 cmdline: 'C:\Users\user\Desktop\PO#4018-308875.pdf.exe' MD5: EA28F2D01808072DBE45804F514EF905)
  - cmd.exe (PID: 6608 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'kolkmjnhgf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\tgfcdsxazs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 6656 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'kolkmjnhgf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\tgfcdsxazs.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - tgfcdsxazs.exe (PID: 6660 cmdline: 'C:\Users\user\AppData\Roaming\tgfcdsxazs.exe' MD5: EA28F2D01808072DBE45804F514EF905)
    - InstallUtil.exe (PID: 3888 cmdline: C:\Users\user\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
00000000.00000002.356654386.000000000430 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6124f:$x1: NanoCore.ClientPluginHost • 0x93e2f:$x1: NanoCore.ClientPluginHost • 0xc69ff:$x1: NanoCore.ClientPluginHost • 0xf95bd:$x1: NanoCore.ClientPluginHost • 0x6128c:$x2: IClientNetworkHost • 0x93e6c:$x2: IClientNetworkHost • 0xc6a3c:$x2: IClientNetworkHost • 0xf95fa:$x2: IClientNetworkHost • 0x64dbf:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x9799f:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xca56f:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xfd12d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.356654386.000000000430 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.356654386.000000000430 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x60fb7:$a: NanoCore • 0x60fc7:$a: NanoCore • 0x611fb:$a: NanoCore • 0x6120f:$a: NanoCore • 0x6124f:$a: NanoCore • 0x93b97:$a: NanoCore • 0x93ba7:$a: NanoCore • 0x93ddb:$a: NanoCore • 0x93def:$a: NanoCore • 0x93e2f:$a: NanoCore • 0xc6767:$a: NanoCore • 0xc6777:$a: NanoCore • 0xc69ab:$a: NanoCore • 0xc69bf:$a: NanoCore • 0xc69ff:$a: NanoCore • 0xf9325:$a: NanoCore • 0xf9335:$a: NanoCore • 0xf9569:$a: NanoCore • 0xf957d:$a: NanoCore • 0xf95bd:$a: NanoCore • 0x61016:$b: ClientPlugin
00000018.00000002.687092112.000000000039 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000018.00000002.687092112.000000000039 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 21 entries				

Unpacked PEs

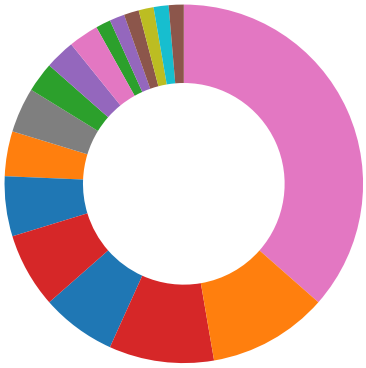
Source	Rule	Description	Author	Strings
24.2.InstallUtil.exe.5150000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
24.2.InstallUtil.exe.5150000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
24.2.InstallUtil.exe.5150000.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
24.2.InstallUtil.exe.4f70000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
24.2.InstallUtil.exe.4f70000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 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
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- 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)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)
- Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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:

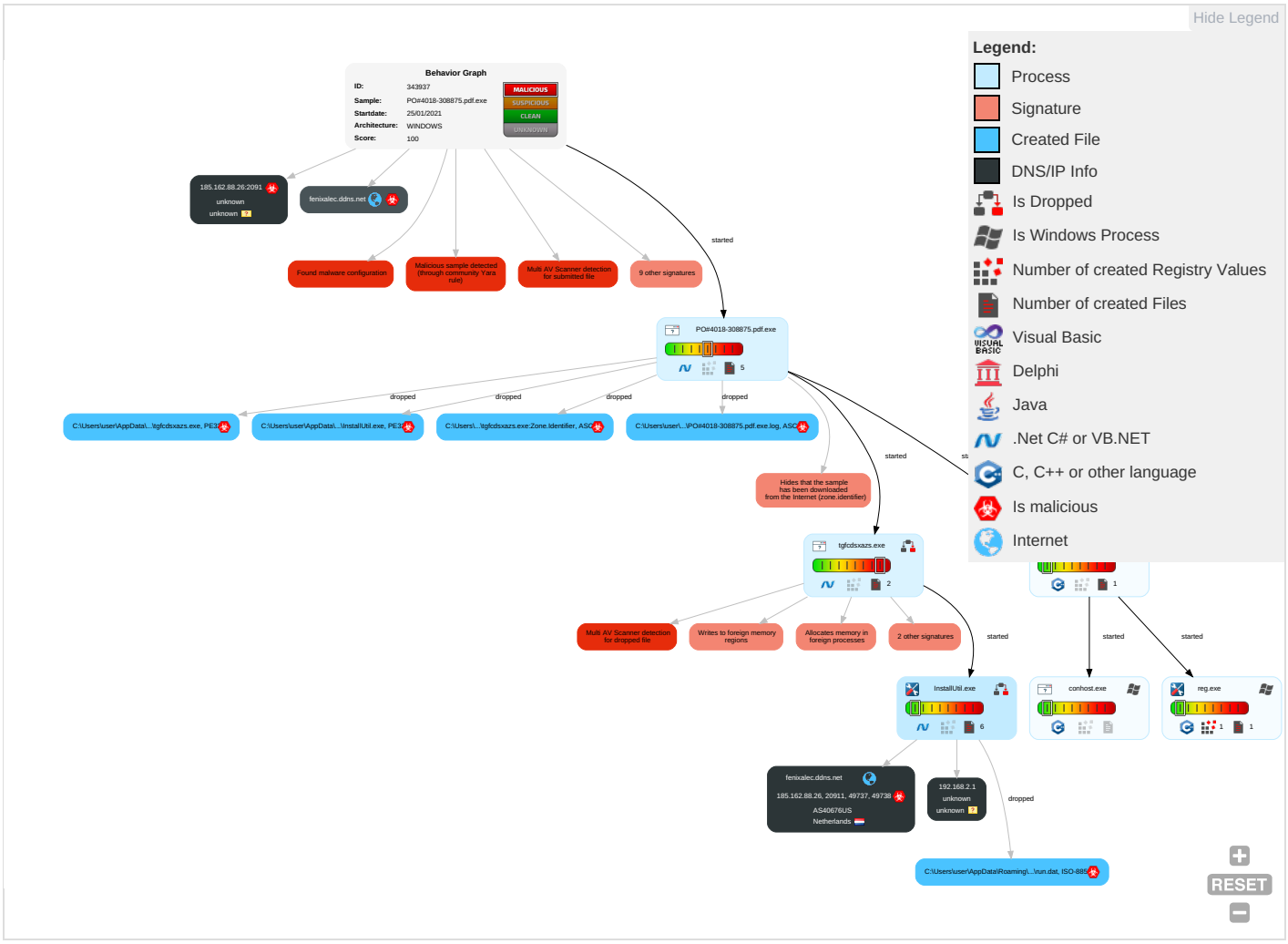
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

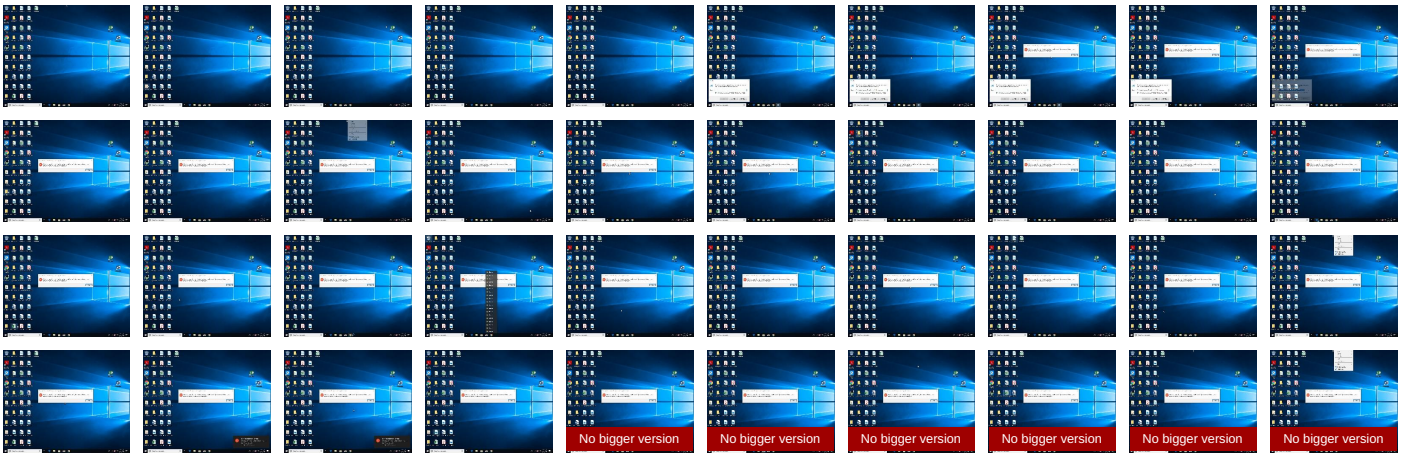
Behavior Graph

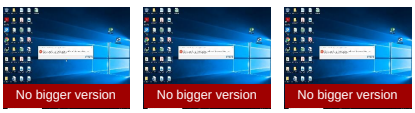


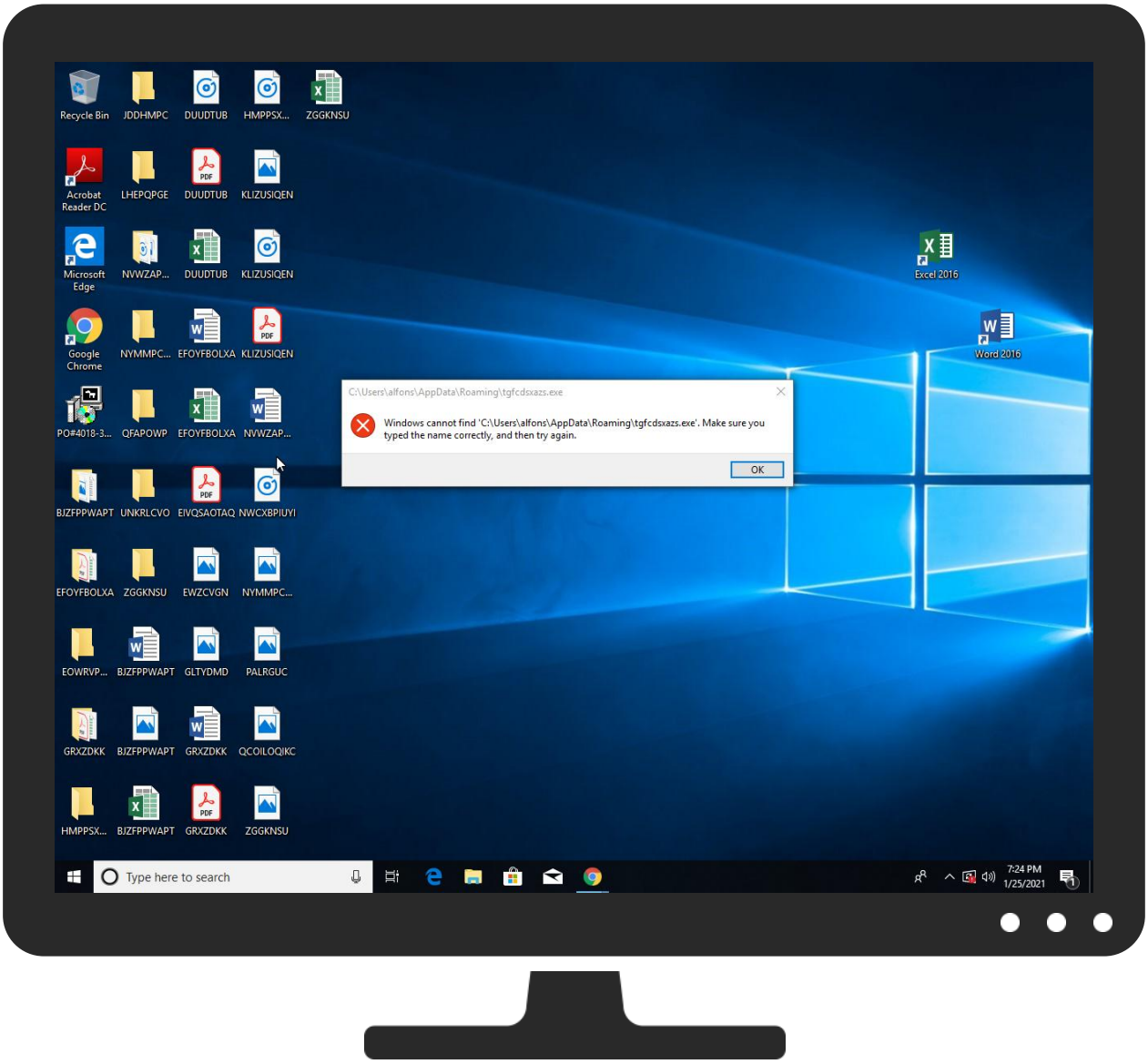
Screenshots

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
PO#4018-308875.pdf.exe	30%	Metadefender		Browse
PO#4018-308875.pdf.exe	67%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\tgfcdsxazs.exe	30%	Metadefender		Browse
C:\Users\user\AppData\Roaming\tgfcdsxazs.exe	67%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.InstallUtil.exe.5150000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
24.2.InstallUtil.exe.390000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

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		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.ado/Ident	tgfcdsxazs.exe, 00000014.00000002.688965801.0000000001789000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.tc4xmp	tgfcdsxazs.exe, 00000014.00000002.688965801.0000000001789000.00000004.00000040.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	343937
Start date:	25.01.2021
Start time:	19:20:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#4018-308875.pdf.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:	34
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@12/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.5%) • Quality average: 39.4% • Quality standard deviation: 37.5%
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 95.101.184.67, 51.104.144.132, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.142.210, 51.103.5.159, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, 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, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.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, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/343937/sample/PO#4018-308875.pdf.exe

Simulations

Behavior and APIs

Time	Type	Description
19:21:18	API Interceptor	208x Sleep call for process: PO#4018-308875.pdf.exe modified
19:21:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kolkmjnhgf C:\Users\user\AppData\Roaming\tgfcdsxazs.exe
19:21:31	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kolkmjnhgf C:\Users\user\AppData\Roaming\tgfcdsxazs.exe
19:22:13	API Interceptor	214x Sleep call for process: tgfcdsxazs.exe modified

Joe Sandbox View / Context

IPs

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

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	file.exe	Get hash	malicious	Browse	
	IMG_5371.EXE	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	IMG_9501.EXE	Get hash	malicious	Browse	
	IMG_04017.pdf.exe	Get hash	malicious	Browse	
	GFS_03781.xls.exe	Get hash	malicious	Browse	
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	
	PO#4018-308875.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#4018-308875.exe	Get hash	malicious	Browse	
	IMG_57880.pdf.exe	Get hash	malicious	Browse	
	PO 67542 PDF.exe	Get hash	malicious	Browse	
	Mi9el6wu1p.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	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.pdf.exe.log	
Process:	C:\Users\user\Desktop\PO#4018-308875.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1053
Entropy (8bit):	5.325704407203577
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84qjE4O1lEE4UVwPKDE4KhK3VZ9pKhp1qE4j:MxHKXfvYHKlEHU0YHKhQnop1qHj
MD5:	3B9C7DC17C94CE377F491CCDC1BDCED7
SHA1:	D20A7E0334D6F6DA612F30E3B07CFF952913D26F
SHA-256:	8578FE540949379FFF261A305EDAB9562D5C6E8148FD07F2A215133E8837C855
SHA-512:	77EFDDAA09B6ED829CE681D49C4767CA985C551A0BE64C5E2041CECBADCAE9645C8E9AB070B512ACB9A01FAA5E6B0F3A3BEEB348C99C4C80F012C1E90A688A8C
Malicious:	**true**
Reputation:	low
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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..2,"System.Drawing, Version=4.0.0.0,

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\PO#4018-308875.pdf.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:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Joe Sandbox View:	• Filename: file.exe, Detection: malicious, Browse • Filename: IMG_5371.EXE, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_9501.EXE, Detection: malicious, Browse • Filename: IMG_04017.pdf.exe, Detection: malicious, Browse • Filename: GFS_03781.xls.exe, Detection: malicious, Browse • Filename: SPpfYOx5Ju.exe, Detection: malicious, Browse • Filename: PO#4018-308875.exe, Detection: malicious, Browse • Filename: PO#4018-308875.exe, Detection: malicious, Browse • 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
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:XNMUn:dt
MD5:	6EBD13D8E407D7E32EA1E3D18A89D4AE
SHA1:	A19612E4D9AB161A31A41926D0F762A9D39B7722
SHA-256:	50EAE76B92449775A23838CAE70A10537AA728AB6543B4822F0E4DA6F78F2EF3
SHA-512:	526007EF589B87F1112807E93BE678A76C63510FEA40CDB28104422C631C02725831FF275A44BC8066D8D2E48C99A1E1F0A151B1405DF9E0E2D6F0BF981FC07A
Malicious:	**true**
Reputation:	low
Preview:	.'C....H

C:\Users\user\AppData\Roaming\tgfcdsxazs.exe	
Process:	C:\Users\user\Desktop\PO#4018-308875.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	642048
Entropy (8bit):	5.385036110771852
Encrypted:	false
SSDEEP:	6144:zE65Gn+cJUsvcfFH+mff7BBTkNAo23KB2pTwcSn9vCfEvgYt:UnVWsvcdHpTkJ23d9ZSn9V9t
MD5:	EA28F2D01808072DBE45804F514EF905
SHA1:	771FF981D42D6C7FC3550DE8CB109E3311B0E0FA
SHA-256:	618D343A6D7F54A0BFD917555C79C6A777B10A35FC2DA0D75F6D85354DE40637
SHA-512:	14C8F4C649F60238A1398BF28CD8A1A1C94D14B74D888A26BCA537317DE1D1BEADA94A6FDB5D51A3AD30EE4C07E389E0FE6EB988E29DF485808FD19114715D 6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 67%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}..... ....@.. ....`.....K.....".....@..@.reloc..... .....@..B.....H.....$.....M.....6.....g...s...?.S.Q..S.5*.LG}x.....6....c.:R..V..H..w../S...!.~..G...|.vd.2.G....M....\.d.X..E.....Q3* ...\.].;...$Yi...2:._...Je...b.B.T:.... .p..KC..5Rj....K..<....5..g..fA...7Q...w.O..^..9...}.....SN.%p...V..@).{..J.9..wO!...w.M....bT.....yb.c..S.G.H.bB..u8B]..2.>i|z..G...A`n=.x..=...+...- ..l...w..3....=..6r..Q:t{..u.8...Q....De.m~w... #.I....;.....S[..KFK,+...O).4....C:.g....cv.}?

C:\Users\user\AppData\Roaming\tgfcdsxazs.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO#4018-308875.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.385036110771852
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:	PO#4018-308875.pdf.exe
File size:	642048
MD5:	ea28f2d01808072dbe45804f514ef905
SHA1:	771ff981d42d6c7fc3550de8cb109e3311b0e0fa
SHA256:	618d343a6d7f54a0bfd917555c79c6a777b10a35fc2da0d75f6d85354de40637
SHA512:	14c8f4c649f60238a1398bf28cd8a1a1c94d14b74d888a26bca537317de1d1beada94a6fdb5d51a3ad30ee4c07e389e0fe6eb988e29df485808fd19114715d16
SSDEEP:	6144:zE65Gn+cJUsvcfFH+mff7BBTkNAo23KB2pTwcSn9vCfEvgYt:UnVWsvcdHpTkJ23d9ZSn9V9t
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...} ....@.. ....` .....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x49dc1e
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:	0x7EAB87D [Mon Mar 18 07:19:25 1974 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General	
File Version Major:	4
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

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
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	0x9dbd0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9e000	0x922	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa0000	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	0x9bc24	0x9be00	False	0.530125426022	data	5.39137035522	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9e000	0x922	0xa00	False	0.39765625	data	4.07942545767	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa0000	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	0x9e130	0x2e8	data		
RT_GROUP_ICON	0x9e418	0x14	data		
RT_VERSION	0x9e42c	0x30c	data		
RT_MANIFEST	0x9e738	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

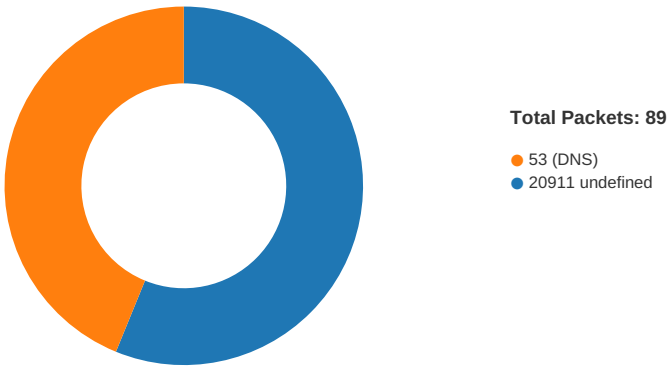
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Mozilla Corporation
FileVersion	30.0
CompanyName	Mozilla Corporation
ProductName	Mozilla Webapp Runtime App Uninstaller
ProductVersion	30.0
FileDescription	Mozilla Webapp Runtime App Uninstaller
OriginalFilename	webapp-uninstaller.exe
Translation	0x0000 0x04b0

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 19:22:50.867099047 CET	49737	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:22:50.917706966 CET	20911	49737	185.162.88.26	192.168.2.5
Jan 25, 2021 19:22:51.432061911 CET	49737	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:22:51.482927084 CET	20911	49737	185.162.88.26	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 19:22:51.994605064 CET	49737	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:22:52.045367956 CET	20911	49737	185.162.88.26	192.168.2.5
Jan 25, 2021 19:22:56.092926025 CET	49738	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:22:56.143428087 CET	20911	49738	185.162.88.26	192.168.2.5
Jan 25, 2021 19:22:56.651403904 CET	49738	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:22:56.701961994 CET	20911	49738	185.162.88.26	192.168.2.5
Jan 25, 2021 19:22:57.213876963 CET	49738	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:22:57.264617920 CET	20911	49738	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:01.406389952 CET	49739	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:01.457076073 CET	20911	49739	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:01.964205980 CET	49739	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:02.014895916 CET	20911	49739	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:02.526880026 CET	49739	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:02.577524900 CET	20911	49739	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:06.753860950 CET	49740	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:06.804553032 CET	20911	49740	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:07.308541059 CET	49740	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:07.359183073 CET	20911	49740	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:07.870935917 CET	49740	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:07.921593904 CET	20911	49740	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:12.043665886 CET	49741	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:12.094314098 CET	20911	49741	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:12.605899096 CET	49741	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:12.656771898 CET	20911	49741	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:13.168265104 CET	49741	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:13.219265938 CET	20911	49741	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:17.384211063 CET	49742	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:17.435059071 CET	20911	49742	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:17.945131063 CET	49742	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:17.995830059 CET	20911	49742	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:18.512541056 CET	49742	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:18.563309908 CET	20911	49742	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:22.578202963 CET	49743	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:22.628803015 CET	20911	49743	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:23.137830019 CET	49743	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:23.188699007 CET	20911	49743	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:23.716943026 CET	49743	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:23.767793894 CET	20911	49743	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:27.795892954 CET	49744	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:27.846633911 CET	20911	49744	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:28.357002020 CET	49744	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:28.407499075 CET	20911	49744	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:28.919524908 CET	49744	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:28.970316887 CET	20911	49744	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:32.985024929 CET	49745	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:33.035639048 CET	20911	49745	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:33.544953108 CET	49745	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:33.595808983 CET	20911	49745	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:34.107724905 CET	49745	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:34.158154964 CET	20911	49745	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:39.211354017 CET	49746	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:39.262022972 CET	20911	49746	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:39.764205933 CET	49746	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:39.815274954 CET	20911	49746	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:40.333091974 CET	49746	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:40.383878946 CET	20911	49746	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:44.491286039 CET	49748	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:44.542066097 CET	20911	49748	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:45.139461040 CET	49748	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:45.190030098 CET	20911	49748	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:45.719048977 CET	49748	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:45.769681931 CET	20911	49748	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:49.851212978 CET	49755	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:49.901854992 CET	20911	49755	185.162.88.26	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 19:23:50.413796902 CET	49755	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:50.464202881 CET	20911	49755	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:50.976363897 CET	49755	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:51.027187109 CET	20911	49755	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:55.045542002 CET	49759	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:55.096136093 CET	20911	49759	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:55.601819038 CET	49759	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:55.652384043 CET	20911	49759	185.162.88.26	192.168.2.5
Jan 25, 2021 19:23:56.164279938 CET	49759	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:23:56.214934111 CET	20911	49759	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:00.230130911 CET	49760	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:00.280808926 CET	20911	49760	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:00.961648941 CET	49760	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:01.012267113 CET	20911	49760	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:01.664941072 CET	49760	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:01.715764046 CET	20911	49760	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:05.728708029 CET	49761	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:05.779441118 CET	20911	49761	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:06.352679968 CET	49761	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:06.403381109 CET	20911	49761	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:06.962107897 CET	49761	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:07.012804985 CET	20911	49761	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:11.260816097 CET	49762	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:11.311621904 CET	20911	49762	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:11.965183020 CET	49762	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:12.015625000 CET	20911	49762	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:12.665815115 CET	49762	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:12.716633081 CET	20911	49762	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:17.383920908 CET	49763	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:17.434721947 CET	20911	49763	185.162.88.26	192.168.2.5
Jan 25, 2021 19:24:17.963021994 CET	49763	20911	192.168.2.5	185.162.88.26
Jan 25, 2021 19:24:18.013741016 CET	20911	49763	185.162.88.26	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 19:21:07.705065012 CET	59596	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:07.752854109 CET	53	59596	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:10.045734882 CET	65296	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:10.104899883 CET	53	65296	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:11.857464075 CET	63183	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:11.905407906 CET	53	63183	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:13.010660887 CET	60151	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:13.058605909 CET	53	60151	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:14.830909967 CET	56969	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:14.878823996 CET	53	56969	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:19.295212984 CET	55161	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:19.349025965 CET	53	55161	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:20.686103106 CET	54757	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:20.734137058 CET	53	54757	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:26.050913095 CET	49992	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:26.111905098 CET	53	49992	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:36.068780899 CET	60075	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:36.119563103 CET	53	60075	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:44.050039053 CET	55016	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:44.113826990 CET	53	55016	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:56.370292902 CET	64345	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:56.429817915 CET	53	64345	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:56.690957069 CET	57128	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:56.778146982 CET	53	57128	8.8.8.8	192.168.2.5
Jan 25, 2021 19:21:57.370459080 CET	54791	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:21:57.434694052 CET	53	54791	8.8.8.8	192.168.2.5
Jan 25, 2021 19:22:00.360069990 CET	50463	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:22:00.419203043 CET	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 19:22:06.393126965 CET	50394	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:22:06.441468000 CET	53	50394	8.8.8.8	192.168.2.5
Jan 25, 2021 19:22:46.629046917 CET	58530	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:22:46.679766893 CET	53	58530	8.8.8.8	192.168.2.5
Jan 25, 2021 19:22:47.088706970 CET	53813	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:22:47.148219109 CET	53	53813	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:06.691986084 CET	63732	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:06.749687910 CET	53	63732	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:11.980174065 CET	57344	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:12.041882992 CET	53	57344	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:17.326075077 CET	54450	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:17.382704973 CET	53	54450	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:39.138854027 CET	59261	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:39.198316097 CET	53	59261	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:44.109695911 CET	57151	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:44.166079044 CET	53	57151	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:44.408252001 CET	59413	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:44.464580059 CET	53	59413	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:44.848939896 CET	60516	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:44.910998106 CET	53	60516	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:45.707304001 CET	51649	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:45.755249023 CET	53	51649	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:46.292948008 CET	65086	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:46.349442959 CET	53	65086	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:47.075252056 CET	56432	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:47.131669044 CET	53	56432	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:47.876236916 CET	52929	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:47.924105883 CET	53	52929	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:48.760588884 CET	64317	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:48.808461905 CET	53	64317	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:49.793334961 CET	61004	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:49.849421024 CET	53	61004	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:50.225378036 CET	56895	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:50.281820059 CET	53	56895	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:51.326426983 CET	62372	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:51.374393940 CET	53	62372	8.8.8.8	192.168.2.5
Jan 25, 2021 19:23:51.827725887 CET	61515	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:23:51.884279966 CET	53	61515	8.8.8.8	192.168.2.5
Jan 25, 2021 19:24:11.195023060 CET	56675	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:24:11.256165981 CET	53	56675	8.8.8.8	192.168.2.5
Jan 25, 2021 19:24:17.276366949 CET	57172	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:24:17.334152937 CET	53	57172	8.8.8.8	192.168.2.5
Jan 25, 2021 19:24:22.657061100 CET	55267	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:24:22.713474035 CET	53	55267	8.8.8.8	192.168.2.5
Jan 25, 2021 19:24:43.700970888 CET	50969	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:24:43.759186983 CET	53	50969	8.8.8.8	192.168.2.5
Jan 25, 2021 19:24:48.951416016 CET	64362	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:24:48.999383926 CET	53	64362	8.8.8.8	192.168.2.5
Jan 25, 2021 19:24:54.200112104 CET	54766	53	192.168.2.5	8.8.8.8
Jan 25, 2021 19:24:54.261842012 CET	53	54766	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 19:23:06.691986084 CET	192.168.2.5	8.8.8.8	0x9f9f	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:11.980174065 CET	192.168.2.5	8.8.8.8	0xf3bc	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:17.326075077 CET	192.168.2.5	8.8.8.8	0x6505	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:39.138854027 CET	192.168.2.5	8.8.8.8	0x9176	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:44.408252001 CET	192.168.2.5	8.8.8.8	0xaa4d	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:49.793334961 CET	192.168.2.5	8.8.8.8	0x4e54	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 19:24:11.195023060 CET	192.168.2.5	8.8.8.8	0xe1ab	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:17.276366949 CET	192.168.2.5	8.8.8.8	0x1099	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:22.657061100 CET	192.168.2.5	8.8.8.8	0xba53	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:43.700970888 CET	192.168.2.5	8.8.8.8	0x46	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:48.951416016 CET	192.168.2.5	8.8.8.8	0x4123	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:54.200112104 CET	192.168.2.5	8.8.8.8	0xdb50	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

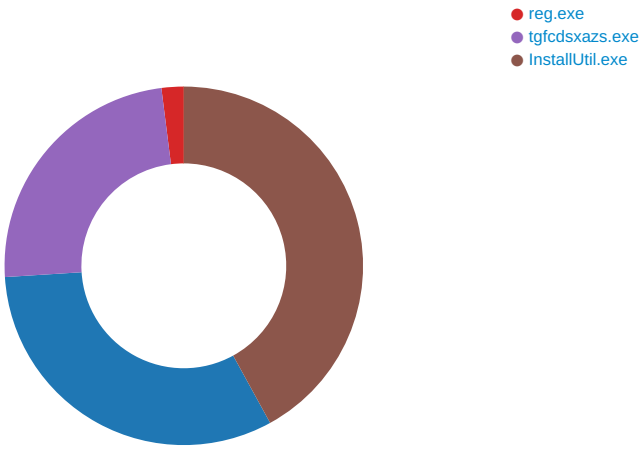
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 19:23:06.749687910 CET	8.8.8.8	192.168.2.5	0x9f9f	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:12.041882992 CET	8.8.8.8	192.168.2.5	0xf3bc	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:17.382704973 CET	8.8.8.8	192.168.2.5	0x6505	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:39.198316097 CET	8.8.8.8	192.168.2.5	0x9176	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:44.464580059 CET	8.8.8.8	192.168.2.5	0xaa4d	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:23:49.849421024 CET	8.8.8.8	192.168.2.5	0x4e54	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:11.256165981 CET	8.8.8.8	192.168.2.5	0xe1ab	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:17.334152937 CET	8.8.8.8	192.168.2.5	0x1099	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:22.713474035 CET	8.8.8.8	192.168.2.5	0xba53	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:43.759186983 CET	8.8.8.8	192.168.2.5	0x46	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:48.999383926 CET	8.8.8.8	192.168.2.5	0x4123	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 25, 2021 19:24:54.261842012 CET	8.8.8.8	192.168.2.5	0xdb50	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- PO#4018-308875.pdf.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: PO#4018-308875.pdf.exe PID: 6520 Parent PID: 5720

General

Start time:	19:21:12
Start date:	25/01/2021
Path:	C:\Users\user\Desktop\PO#4018-308875.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO#4018-308875.pdf.exe'
Imagebase:	0xe80000
File size:	642048 bytes
MD5 hash:	EA28F2D01808072DBE45804F514EF905
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: 00000000.00000002.356654386.0000000004301000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.356654386.0000000004301000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.356654386.0000000004301000.00000004.00000001.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\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	595E9FB	CopyFileExW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tgfcdsxazs.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	595E9FB	CopyFileExW
C:\Users\user\AppData\Roaming\tgfcdsxazs.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	595E9FB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFAC78D	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 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 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z......... ....0..T...........r... ....@.. ....`................	success or wait	1	595E9FB	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tgfcdsxazs.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 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 7d b8 ea 07 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 be 09 00 00 0c 00 00 00 00 00 00 1e dc 09 00 00 20 00 00 00 e0 09 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 20 0a 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...}............ ....@.. ....`................	success or wait	3	595E9FB	CopyFileExW
C:\Users\user\AppData\Roaming\ tgfcdsxazs.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	595E9FB	CopyFileExW
C:\Users\user\AppData\Local\Mi crosoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.pdf.exe.log	unknown	1053	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	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..2,"Microsoft. VisualBasic, Ver	success or wait	1	6DFAC907	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	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	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	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile

Analysis Process: cmd.exe PID: 6608 Parent PID: 6520

General

Start time:	19:21:17
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'kolkmjnhgf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\tgfcdsxazs.exe'
Imagebase:	0xe30000
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: 6616 Parent PID: 6608

General

Start time:	19:21:17
Start date:	25/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6656 Parent PID: 6608

General

Start time:	19:21:17
Start date:	25/01/2021

Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'kolkmjnhgf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\tgfcdsxazs.exe'
Imagebase:	0x810000
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	kolkmjnhgf	unicode	C:\Users\user\AppData\Roaming\tgfcdsxazs.exe	success or wait	1	815A1D	RegSetValueExW

Analysis Process: tgfcdsxazs.exe PID: 6660 Parent PID: 6520

General

Start time:	19:22:07
Start date:	25/01/2021
Path:	C:\Users\user\AppData\Roaming\tgfcdsxazs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tgfcdsxazs.exe'
Imagebase:	0xcd0000
File size:	642048 bytes
MD5 hash:	EA28F2D01808072DBE45804F514EF905
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: 00000014.00000002.696946485.0000000004B14000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.696946485.0000000004B14000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.696946485.0000000004B14000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.696822953.0000000004A81000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.696822953.0000000004A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.696822953.0000000004A81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 30%, Metadefender, Browse • Detection: 67%, ReversingLabs
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	6DC9CF06	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	6DC9CF06	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	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5a e0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationC ore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown

Analysis Process: InstallUtil.exe PID: 3888 Parent PID: 6660

General

Start time:	19:22:43
Start date:	25/01/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x2c0000
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: 00000018.00000002.687092112.0000000000392000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.687092112.0000000000392000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.687092112.0000000000392000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.697105456.0000000004F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.697105456.0000000004F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.697259526.0000000005150000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.697259526.0000000005150000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.697259526.0000000005150000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.694427019.0000000003759000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.694427019.0000000003759000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• 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	6DC9CF06	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	6DC9CF06	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	6CAEBEFF	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	6CAE1E60	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	6CAEBEFF	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	6CAEBEFF	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	dc 27 43 a8 a9 c1 d8 48	.'C....H	success or wait	1	6CAE1B4F	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	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	4096	success or wait	1	6DC5D72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	512	success or wait	1	6DC5D72F	unknown

Disassembly

Code Analysis