ID: 341926
Sample Name: PO#4018-308875.pdf.exe
Cookbook: default.jbs
Time: 07:29:15
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

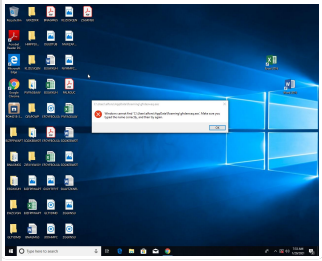
Analysis Report PO#4018-308875.pdf.exe

Overview

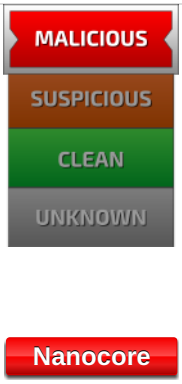
General Information

Sample Name:	PO#4018-308875.pdf.exe
Analysis ID:	341926
MD5:	d90049e2aff3035..
SHA1:	1153f298db7e6ae.
SHA256:	761e77be2bbf608.
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



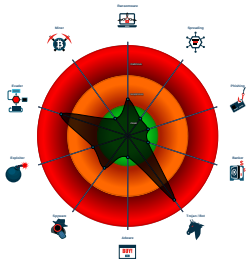
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- 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…

Classification



Startup

- **System is w10x64**
- PO#4018-308875.pdf.exe (PID: 6080 cmdline: 'C:\Users\user\Desktop\PO#4018-308875.pdf.exe' MD5: D90049E2AFF303588E499820E0D9078C)
  - cmd.exe (PID: 5444 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'olkkmmxxzaa' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\gfrdeswaq.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 4636 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'olkkmmxxzaa' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\gfrdeswaq.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - gfrdeswaq.exe (PID: 6764 cmdline: 'C:\Users\user\AppData\Roaming\gfrdeswaq.exe' MD5: D90049E2AFF303588E499820E0D9078C)
    - InstallUtil.exe (PID: 6280 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: NanoCore


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000002.618309984.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000019.00000002.618309984.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000019.00000002.618309984.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000019.00000002.628566138.000000000501 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000019.00000002.628566138.000000000501 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
25.2.InstallUtil.exe.5010000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
25.2.InstallUtil.exe.5010000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
25.2.InstallUtil.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
25.2.InstallUtil.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
25.2.InstallUtil.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 7 entries				

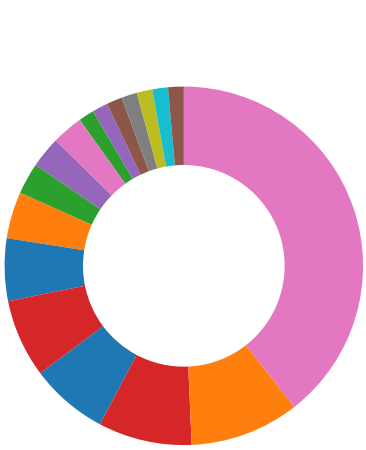
Sigma Overview

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



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)
- .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)
- Uses an obfuscated file name to hide its real file extension (double extension)

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:

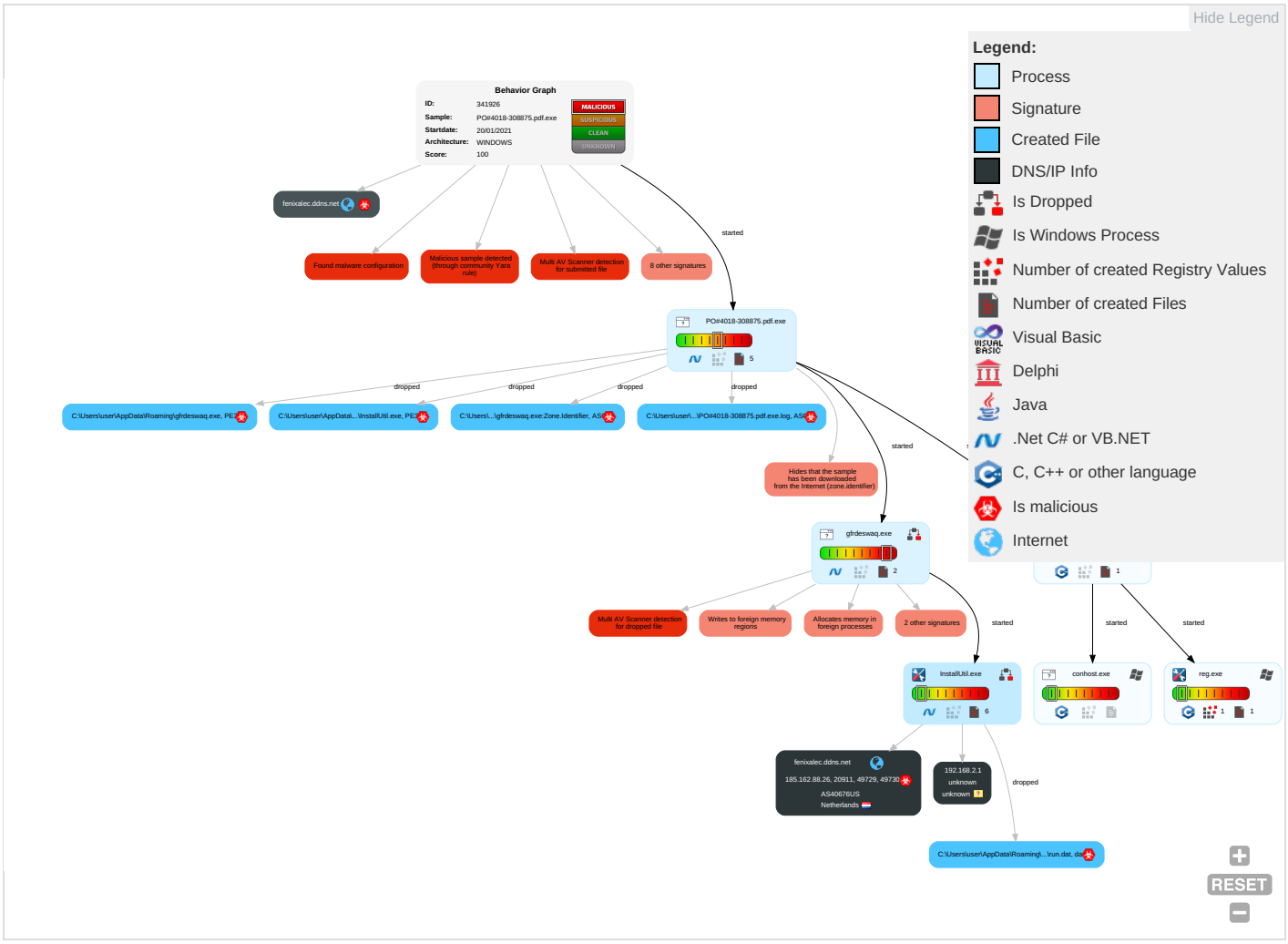
Detected Nanocore Rat

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 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 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 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-Applica 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	Applica 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	Applica Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 1 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

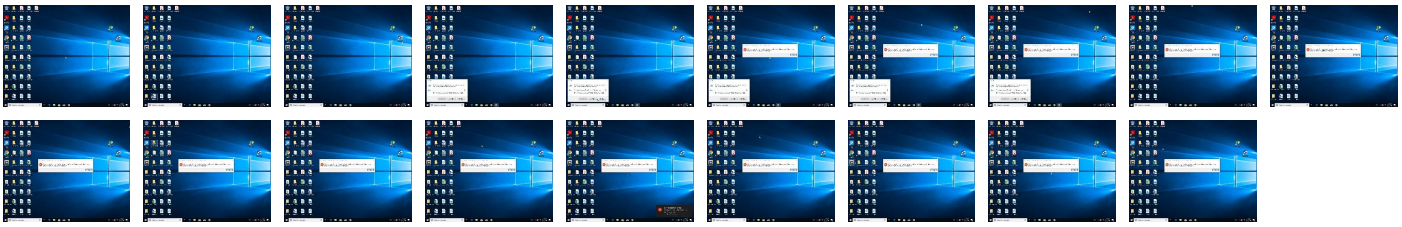
Behavior Graph

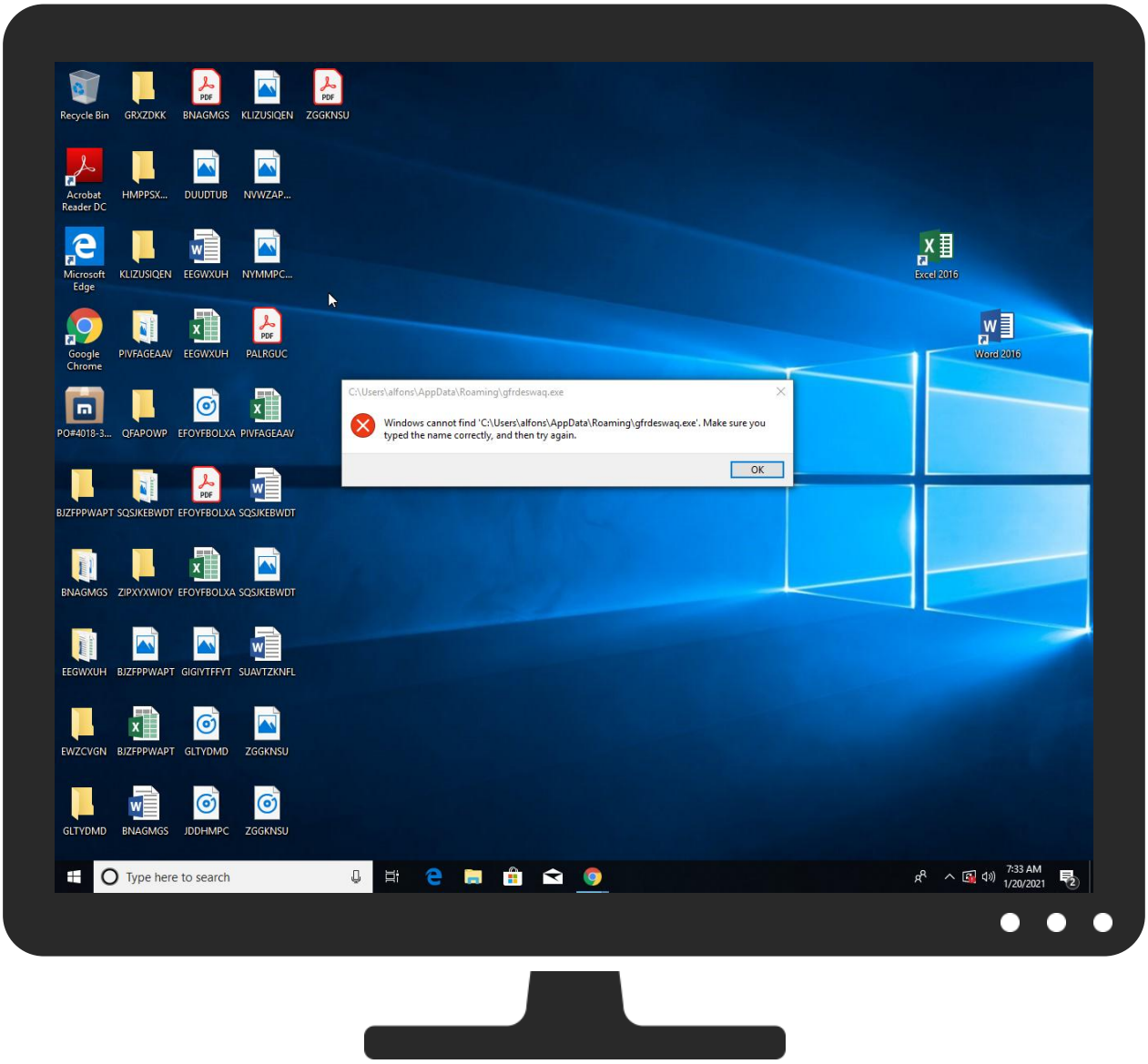


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO#4018-308875.pdf.exe	15%	ReversingLabs	Win32.Trojan.Wacatac	

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\gfrdeswaq.exe	15%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
25.2.InstallUtil.exe.5220000.6.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	

Domains and IPs

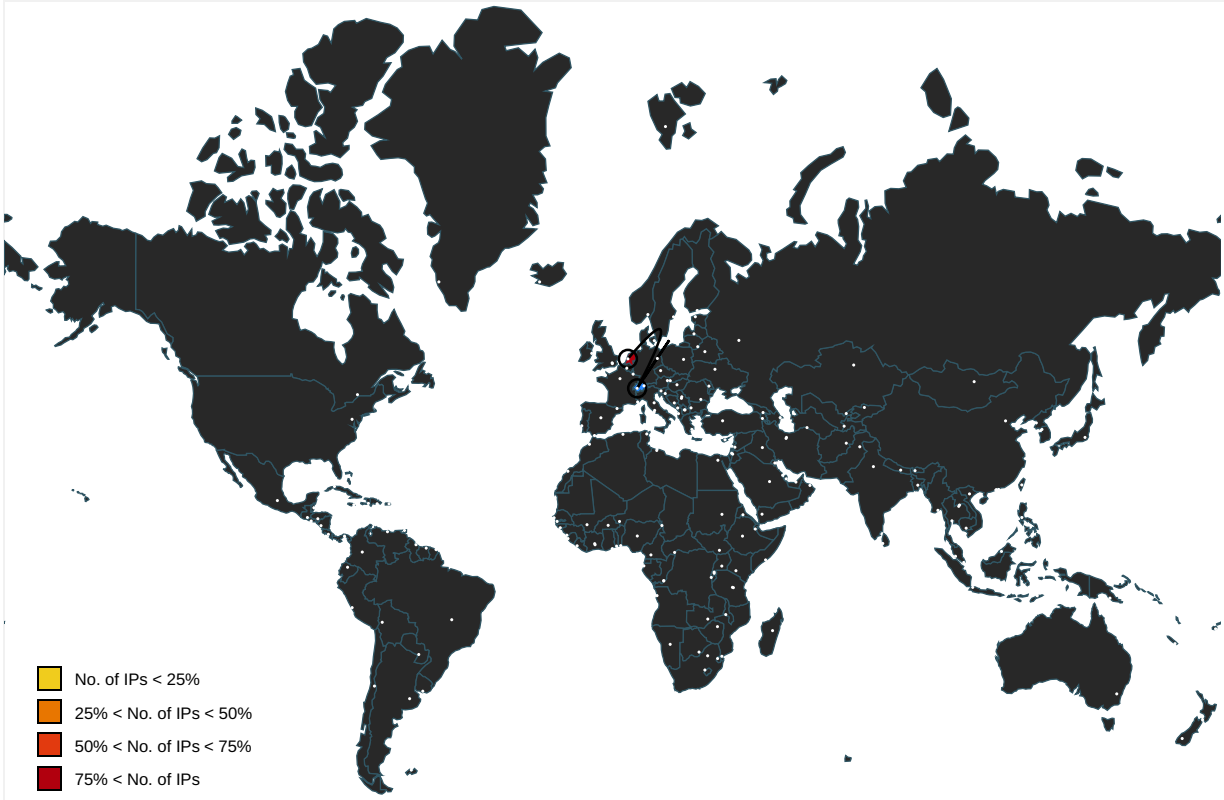
Contacted Domains

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.pdf.exe, 00000000.00000003.331443931.00000000014C9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond

Analysis ID:	341926
Start date:	20.01.2021
Start time:	07:29:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 19s
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:	35
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: 0.4% (good quality ratio 0.1%) • Quality average: 18.2% • Quality standard deviation: 32.6%
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, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 40.88.32.150, 51.104.139.180, 92.122.213.247, 92.122.213.194, 51.103.5.186, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, par02p.wns.notify.trafficmanager.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
07:30:11	API Interceptor	201x Sleep call for process: PO#4018-308875.pdf.exe modified
07:30:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run olkkmmxxzaa C:\Users\user\AppData\Roaming\gfrdeswaq.exe
07:30:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run olkkmmxxzaa C:\Users\user\AppData\Roaming\gfrdeswaq.exe
07:31:03	API Interceptor	200x Sleep call for process: gfrdeswaq.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.162.88.26	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	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	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	• 172.106.111.244
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 104.149.57.92
	SWIFT-COPY Payment advice3243343.exe	Get hash	malicious	Browse	• 172.106.111.244
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 107.160.127.252
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 107.160.127.252
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 107.160.127.252
	NPD76122.exe	Get hash	malicious	Browse	• 104.217.231.247
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 104.217.231.248
	d2mISAbTQN.exe	Get hash	malicious	Browse	• 104.217.231.248
	n41pVXkYCe.exe	Get hash	malicious	Browse	• 104.217.231.248
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 104.217.231.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	53McmgaUJP.exe	Get hash	malicious	Browse	• 104.217.231.248
	BsR85tOyjL.exe	Get hash	malicious	Browse	• 104.217.231.248

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	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	
	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	
	IMG_71103.pdf.exe	Get hash	malicious	Browse	
	WjIKk3FzeI.exe	Get hash	malicious	Browse	
	iv2yPzJEMs.exe	Get hash	malicious	Browse	
	Jb4NE4iWz5.exe	Get hash	malicious	Browse	
	mmcrkHjIb3.exe	Get hash	malicious	Browse	
	fkGmyP7ryc.exe	Get hash	malicious	Browse	
	product supplies 10589TW.exe	Get hash	malicious	Browse	
	IMG_13791.pdf.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):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895EABB
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..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.pdf.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
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: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• 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 • Filename: IMG_71103.pdf.exe, Detection: malicious, Browse • Filename: WjIKk3FzeI.exe, Detection: malicious, Browse • Filename: iv2yPzJEMs.exe, Detection: malicious, Browse • Filename: Jb4NE4iWz5.exe, Detection: malicious, Browse • Filename: mmcrkHjIb3.exe, Detection: malicious, Browse • Filename: fkGmyP7ryc.exe, Detection: malicious, Browse • Filename: product supplies 10589TW.exe, Detection: malicious, Browse • Filename: IMG_13791.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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:I6P:Iq
MD5:	67B9DD027EDDE081BABBBB3F21F38634
SHA1:	8D78824EB573B5241A92587DDA5BE4ABB877C66D
SHA-256:	3A71BB34D6D0B9075ED5F864C16300AF74B34FE99A32A60EC212001830F4F3EC
SHA-512:	6DC3178E91AD6653B0426D950F0E6A2ED52484D61FCC51CD0AF5FBD99EDFA6FFD9E9DE92BA1F4B851440406EBAECFA02CF92CF0F8ADA8ACD17C6C35E363E6AC
Malicious:	**true**
Reputation:	low
Preview:	...zX..H

C:\Users\user\AppData\Roaming\gfrdeswaq.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):	783360
Entropy (8bit):	5.789061235197813
Encrypted:	false
SSDEEP:	12288:NAagt50jwcEc6tvHpTkJ23d9ZSn9V9ovGPfiu:N3i08cEc6tvHpAIZSnb+vGXi
MD5:	D90049E2AFF303588E499820E0D9078C
SHA1:	1153F298DB7E6AEED9C3A55C907DFA474AE9155F
SHA-256:	761E77BE2BBF6089F04B1901C44548BD4FF5AC873A74B1CA0E0604BB902EFF22
SHA-512:	0AB4D1CCD24FA3174750B69F929C8DC34334F88941F1708E5EDC2FDB7498636AA0C441BB9BB7E54A1EBB246500DDBFDDBDBCCFD4FE1EC7EE16C14229AF1F9E89
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%

C:\Users\user\AppData\Roaming\gfrdeswaq.exe	
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-.D\.....^..... .....@.. .....@..... ..`.....K.....N[..... ..... ..... ..H.....text..... ..... ..`.rsrc...N[.....\.....@..@.reloc..... .....@..B.....H.....x...:.....C....B...6.....V.=y.....N..>..y..:..#..1.[...:.....SD8....F.=...6ix..D.J.....{....-.=..g..Y.....p";.....}....M. .....^.}.1..BX..t.,.|.>.B..v$j.V..v.o<i]s.(.).1.....-\..~..N!%..;v.@.3...?.6u...c".1.3p.^.....F.....r..%.o.....L..F.....@[...`.~.....@o.#..P..5.Y....?..s~x.2V....|...z8.r%l.b.....6.....^r.!!.. ....F....+Au...:uxr.;..x.=...xI..@K....uc.$..P.!AS.e.w.D .I....{...I..q/...6...

C:\Users\user\AppData\Roaming\gfrdeswaq.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO#4018-308875.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.789061235197813
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:	783360
MD5:	d90049e2aff303588e499820e0d9078c
SHA1:	1153f298db7e6aeed9c3a55c907dfa474ae9155f
SHA256:	761e77be2bbf6089f04b1901c44548bd4ff5ac873a74b1ca0e0604bb902eff22
SHA512:	0ab4d1ccd24fa3174750b69f929c8dc34334f88941f1708e5edc2fdb7498636aa0c441bb9bb7e54a1ebb246500ddbddbdbccfd4fe1ec7ee16c14229af1f9e89
SSDEEP:	12288:NAagt50jwcEc6tvHpTkJ23d9ZSn9V9ovGPfiu:N3i08cEc6tvHpAIZSnb+vGXi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-.D\.....^..... .....@.. .....@..... ...`.....

File Icon

Icon Hash:	b2718f33292b177e

Static PE Info

General

Entrypoint:	0x4ab2fe
Entrypoint Section:	.text

General

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:	0x5C44F42D [Sun Jan 20 22:20:29 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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	0xab2b0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x15b4e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xa9304	0xa9400	False	0.526561923006	data	5.51757303939	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x15b4e	0x15c00	False	0.631824712644	data	7.26106977005	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xac370	0x2e8	data		
RT_ICON	0xac658	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0xac780	0xea8	data		
RT_ICON	0xad628	0x8a8	data		
RT_ICON	0xaded0	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xae438	0x889f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb6cd8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 224, next used block 117440512		
RT_ICON	0xbaf00	0x25a8	data		
RT_ICON	0xbd4a8	0x1a68	data		
RT_ICON	0xbef10	0x10a8	data		
RT_ICON	0xbffb8	0x988	data		
RT_ICON	0xc0940	0x6b8	data		
RT_ICON	0xc0ff8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc1460	0xbc	data		
RT_VERSION	0xc151c	0x448	data	English	United States
RT_MANIFEST	0xc1964	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

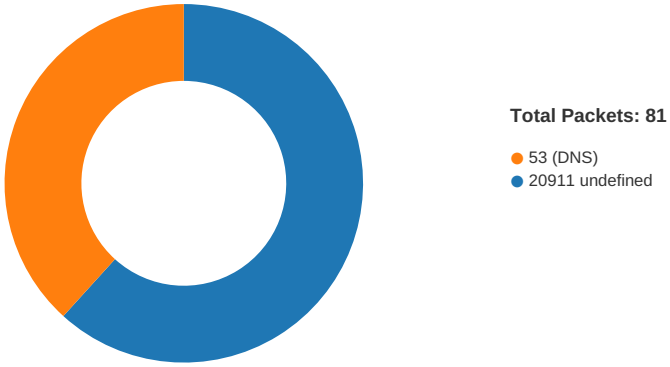
Description	Data
LegalCopyright	Copyright 2020 Maxthon Ltd. All rights reserved.
InternalName	mini_installer
CompanyShortName	Maxthon Ltd.
FileVersion	6.1.0.2000
CompanyName	Maxthon Ltd.
ProductShortName	Maxthon Installer
ProductName	Maxthon Installer
LastChange	94abc2237ae0c9a4cb5f035431c8adfb94324633-refs/branch-heads/4183@{#1658}
ProductVersion	6.1.0.2000
FileDescription	Maxthon Installer
Official Build	1
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 07:31:39.854502916 CET	49729	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:39.905483007 CET	20911	49729	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:40.408859015 CET	49729	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:40.459676027 CET	20911	49729	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:40.971297979 CET	49729	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:41.021905899 CET	20911	49729	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:45.101613045 CET	49730	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:45.152352095 CET	20911	49730	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:45.659298897 CET	49730	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:45.709918976 CET	20911	49730	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:46.221895933 CET	49730	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:46.272509098 CET	20911	49730	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:50.286111116 CET	49731	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:50.336662054 CET	20911	49731	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:50.847104073 CET	49731	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:50.897509098 CET	20911	49731	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:51.409755945 CET	49731	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:51.460391998 CET	20911	49731	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:55.742108107 CET	49732	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:55.792807102 CET	20911	49732	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:56.300697088 CET	49732	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:56.351223946 CET	20911	49732	185.162.88.26	192.168.2.5
Jan 20, 2021 07:31:56.863302946 CET	49732	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:31:56.914103985 CET	20911	49732	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:00.993782043 CET	49733	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:01.044477940 CET	20911	49733	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:01.551114082 CET	49733	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:01.601830006 CET	20911	49733	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:02.113833904 CET	49733	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:02.164552927 CET	20911	49733	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:06.242758989 CET	49734	20911	192.168.2.5	185.162.88.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 07:32:06.293401957 CET	20911	49734	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:06.801650047 CET	49734	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:06.852528095 CET	20911	49734	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:07.364125967 CET	49734	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:07.414671898 CET	20911	49734	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:11.428158998 CET	49735	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:11.478652000 CET	20911	49735	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:11.989595890 CET	49735	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:12.040324926 CET	20911	49735	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:12.552088976 CET	49735	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:12.602437019 CET	20911	49735	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:16.616096973 CET	49736	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:16.666659117 CET	20911	49736	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:17.177428007 CET	49736	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:17.228347063 CET	20911	49736	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:17.740000010 CET	49736	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:17.790555000 CET	20911	49736	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:21.806370974 CET	49737	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:21.857095957 CET	20911	49737	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:22.365370035 CET	49737	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:22.416100025 CET	20911	49737	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:22.927898884 CET	49737	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:22.978466034 CET	20911	49737	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:27.107625961 CET	49738	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:27.158226967 CET	20911	49738	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:27.662640095 CET	49738	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:27.713306904 CET	20911	49738	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:28.225193977 CET	49738	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:28.275882006 CET	20911	49738	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:32.402971983 CET	49739	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:32.453649998 CET	20911	49739	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:32.961524963 CET	49739	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:33.012324095 CET	20911	49739	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:33.522510052 CET	49739	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:33.573262930 CET	20911	49739	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:37.712385893 CET	49740	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:37.763009071 CET	20911	49740	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:38.302246094 CET	49740	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:38.352889061 CET	20911	49740	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:38.992669106 CET	49740	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:39.043415070 CET	20911	49740	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:43.051678896 CET	49746	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:43.102233887 CET	20911	49746	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:43.608247995 CET	49746	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:43.658893108 CET	20911	49746	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:44.170759916 CET	49746	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:44.221250057 CET	20911	49746	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:48.235095024 CET	49752	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:48.285700083 CET	20911	49752	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:48.796133995 CET	49752	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:48.846766949 CET	20911	49752	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:49.358694077 CET	49752	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:49.409111977 CET	20911	49752	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:53.422578096 CET	49753	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:53.473304987 CET	20911	49753	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:53.984086990 CET	49753	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:54.034677029 CET	20911	49753	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:54.546641111 CET	49753	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:54.597167969 CET	20911	49753	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:58.883698940 CET	49754	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:58.934469938 CET	20911	49754	185.162.88.26	192.168.2.5
Jan 20, 2021 07:32:59.437683105 CET	49754	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:32:59.488444090 CET	20911	49754	185.162.88.26	192.168.2.5
Jan 20, 2021 07:33:00.000999928 CET	49754	20911	192.168.2.5	185.162.88.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 07:33:00.051909924 CET	20911	49754	185.162.88.26	192.168.2.5
Jan 20, 2021 07:33:04.554666996 CET	49755	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:33:04.605324984 CET	20911	49755	185.162.88.26	192.168.2.5
Jan 20, 2021 07:33:05.110050917 CET	49755	20911	192.168.2.5	185.162.88.26
Jan 20, 2021 07:33:05.160808086 CET	20911	49755	185.162.88.26	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 07:30:00.328669071 CET	59596	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:00.387139082 CET	53	59596	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:01.378868103 CET	65296	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:01.429608107 CET	53	65296	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:02.159115076 CET	63183	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:02.207123995 CET	53	63183	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:03.067598104 CET	60151	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:03.115561008 CET	53	60151	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:15.570496082 CET	56969	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:15.618387938 CET	53	56969	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:16.518938065 CET	55161	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:16.577927113 CET	53	55161	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:30.826376915 CET	54757	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:30.875653028 CET	53	54757	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:36.568918943 CET	49992	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:36.629512072 CET	53	49992	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:49.575465918 CET	60075	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:49.626271963 CET	53	60075	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:50.580446005 CET	55016	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:50.644397020 CET	53	55016	8.8.8.8	192.168.2.5
Jan 20, 2021 07:30:53.665081978 CET	64345	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:30:53.721483946 CET	53	64345	8.8.8.8	192.168.2.5
Jan 20, 2021 07:31:27.587776899 CET	57128	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:31:27.635565996 CET	53	57128	8.8.8.8	192.168.2.5
Jan 20, 2021 07:31:55.679936886 CET	54791	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:31:55.738428116 CET	53	54791	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:00.930579901 CET	50463	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:00.991537094 CET	53	50463	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:06.184623957 CET	50394	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:06.241209984 CET	53	50394	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:27.046736956 CET	58530	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:27.105943918 CET	53	58530	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:32.341784000 CET	53813	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:32.401135921 CET	53	53813	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:37.644326925 CET	63732	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:37.700372934 CET	53	63732	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:39.441392899 CET	57344	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:39.492288113 CET	53	57344	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:40.285835981 CET	54450	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:40.342093945 CET	53	54450	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:41.056921959 CET	59261	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:41.115889072 CET	53	59261	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:41.594192982 CET	57151	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:41.650599957 CET	53	57151	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:42.263398886 CET	59413	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:42.319693089 CET	53	59413	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:43.092466116 CET	60516	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:43.140361071 CET	53	60516	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:43.907529116 CET	51649	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:43.963603973 CET	53	51649	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:45.203284025 CET	65086	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:45.251498938 CET	53	65086	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:46.543776035 CET	56432	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:46.591660976 CET	53	56432	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:48.046406984 CET	52929	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 07:32:48.094095945 CET	53	52929	8.8.8.8	192.168.2.5
Jan 20, 2021 07:32:58.664227962 CET	64317	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:32:58.720607042 CET	53	64317	8.8.8.8	192.168.2.5
Jan 20, 2021 07:33:04.489262104 CET	61004	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:33:04.547322035 CET	53	61004	8.8.8.8	192.168.2.5
Jan 20, 2021 07:33:09.955523014 CET	56895	53	192.168.2.5	8.8.8.8
Jan 20, 2021 07:33:10.016967058 CET	53	56895	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2021 07:31:55.679936886 CET	192.168.2.5	8.8.8.8	0xe915	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:00.930579901 CET	192.168.2.5	8.8.8.8	0x85be	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:06.184623957 CET	192.168.2.5	8.8.8.8	0xc998	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:27.046736956 CET	192.168.2.5	8.8.8.8	0xcce3	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:32.341784000 CET	192.168.2.5	8.8.8.8	0xa8b6	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:37.644326925 CET	192.168.2.5	8.8.8.8	0xa38c	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:58.664227962 CET	192.168.2.5	8.8.8.8	0x60c2	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:33:04.489262104 CET	192.168.2.5	8.8.8.8	0x1fd9	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 07:33:09.955523014 CET	192.168.2.5	8.8.8.8	0x96aa	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

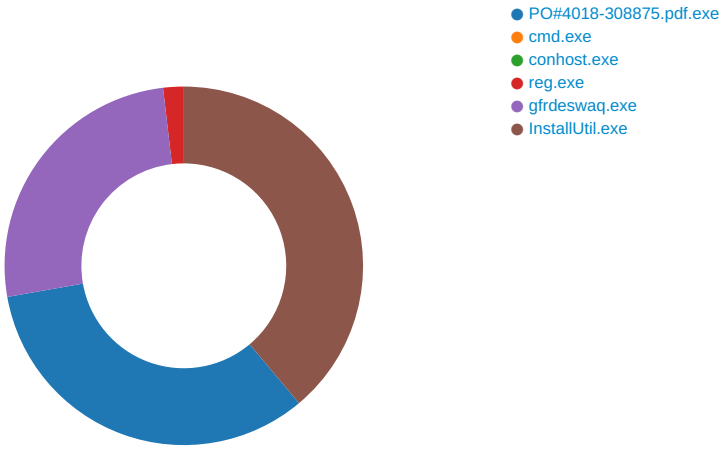
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 07:31:55.738428116 CET	8.8.8.8	192.168.2.5	0xe915	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:00.991537094 CET	8.8.8.8	192.168.2.5	0x85be	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:06.241209984 CET	8.8.8.8	192.168.2.5	0xc998	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:27.105943918 CET	8.8.8.8	192.168.2.5	0xcce3	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:32.401135921 CET	8.8.8.8	192.168.2.5	0xa8b6	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:37.700372934 CET	8.8.8.8	192.168.2.5	0xa38c	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:32:58.720607042 CET	8.8.8.8	192.168.2.5	0x60c2	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:33:04.547322035 CET	8.8.8.8	192.168.2.5	0x1fd9	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 20, 2021 07:33:10.016967058 CET	8.8.8.8	192.168.2.5	0x96aa	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PO#4018-308875.pdf.exe PID: 6080 Parent PID: 5628

General

Start time:	07:30:05
Start date:	20/01/2021
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:	0x9d0000
File size:	783360 bytes
MD5 hash:	D90049E2AFF303588E499820E0D9078C
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: 00000000.00000002.337437485.0000000004734000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.337437485.0000000004734000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.337437485.0000000004734000.00000004.00000001.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	550EE1B	CopyFileExW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gfrdeswaq.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	550EE1B	CopyFileExW
C:\Users\user\AppData\Roaming\gfrdeswaq.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	550EE1B	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 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 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....Z.Z..... ....0..T.....r... .....@.. ....`.....	success or wait	1	550EE1B	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gfrdeswaq.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 2d f4 44 5c 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 94 0a 00 00 5e 01 00 00 00 00 00 fe b2 0a 00 00 20 00 00 00 c0 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 0c 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...- .D\....................^.......... ....@.. ....@ ....`................	success or wait	3	550EE1B	CopyFileExW
C:\Users\user\AppData\Roaming\ gfrdeswaq.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	550EE1B	CopyFileExW
C:\Users\user\AppData\Local\Mi crosoft\CLR_v4.0_32\UsageLogs\PO#4018- 308875.pdf.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	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\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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	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
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DBD03DE	ReadFile

Analysis Process: cmd.exe PID: 5444 Parent PID: 6080

General

Start time:	07:30:09
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'olkkmmxxzaa' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\gfrdeswaq.exe'
Imagebase:	0x150000
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: 5952 Parent PID: 5444

General

Start time:	07:30:10
Start date:	20/01/2021
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: 4636 Parent PID: 5444

General

Start time:	07:30:10
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'olkkmmxxzaa' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\gfrdeswaq.exe'
Imagebase:	0x1320000
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	olkkmmxxzaa	unicode	C:\Users\user\AppData\Roaming\gfrdeswaq.exe	success or wait	1	1325A1D	RegSetValueExW

Analysis Process: gfrdeswaq.exe PID: 6764 Parent PID: 6080

General

Start time:	07:30:55
Start date:	20/01/2021
Path:	C:\Users\user\AppData\Roaming\gfrdeswaq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\gfrdeswaq.exe'
Imagebase:	0xe50000
File size:	783360 bytes
MD5 hash:	D90049E2AFF303588E499820E0D9078C
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: 00000014.00000002.627989417.0000000004C62000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.627989417.0000000004C62000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.627989417.0000000004C62000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.627812499.0000000004BCF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.627812499.0000000004BCF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.627812499.0000000004BCF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 15%, 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\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\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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	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
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	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: 6280 Parent PID: 6764

General

Start time:	07:31:33
Start date:	20/01/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x500000
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: 00000019.00000002.618309984.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.618309984.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.618309984.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000002.628566138.0000000005010000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000019.00000002.628566138.0000000005010000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.621682158.0000000002971000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000002.628917829.0000000005220000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000019.00000002.628917829.0000000005220000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.628917829.0000000005220000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.625511486.00000000039B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.625511486.00000000039B9000.00000004.00000001.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	f3 1a ee 7a 58 bd d8 48	...zX..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\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\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	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
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\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