ID: 342480
Sample Name: PO#4018-308875.exe
Cookbook: default.jbs
Time: 07:22:36
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

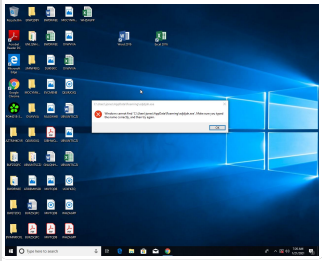
Analysis Report PO#4018-308875.exe

Overview

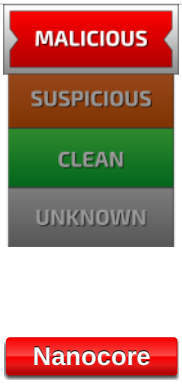
General Information

Sample Name:	PO#4018-308875.exe
Analysis ID:	342480
MD5:	37bb301570706e..
SHA1:	9ff8d1dcca0c34f…
SHA256:	4e599dda2d5d0f3.
Tags:	exe

Most interesting Screenshot:



Detection



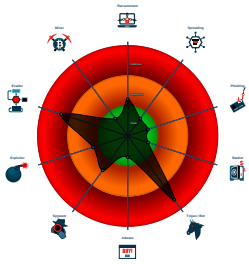
Nanocore

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

Signatures

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

Classification



Startup

- **System is w10x64**
- PO#4018-308875.exe (PID: 4780 cmdline: 'C:\Users\user\Desktop\PO#4018-308875.exe' MD5: 37BB301570706E9B086C26C16E7CDB83)
  - cmd.exe (PID: 3220 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'vsg63637' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\edjdjdn.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 5760 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'vsg63637' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\edjdjdn.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - edjdjdn.exe (PID: 2016 cmdline: 'C:\Users\user\AppData\Roaming\edjdjdn.exe' MD5: 37BB301570706E9B086C26C16E7CDB83)
    - InstallUtil.exe (PID: 5480 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
0000000E.00000002.1087650939.00000000042 4A000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x11007:$x1: NanoCore.ClientPluginHost • 0x43bbd:$x1: NanoCore.ClientPluginHost • 0x11044:$x2: IClientNetworkHost • 0x43bfa:$x2: IClientNetworkHost • 0x14b77:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4772d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.1087650939.00000000042 4A000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000002.1087650939.00000000042 4A000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10d6f:$a: NanoCore • 0x10d7f:$a: NanoCore • 0x10fb3:$a: NanoCore • 0x10fc7:$a: NanoCore • 0x11007:$a: NanoCore • 0x43925:$a: NanoCore • 0x43935:$a: NanoCore • 0x43b69:$a: NanoCore • 0x43b7d:$a: NanoCore • 0x43bbd:$a: NanoCore • 0x10dce:$b: ClientPlugin • 0x10fd0:$b: ClientPlugin • 0x11010:$b: ClientPlugin • 0x43984:$b: ClientPlugin • 0x43b86:$b: ClientPlugin • 0x43bc6:$b: ClientPlugin • 0x10ef5:$c: ProjectData • 0x43aab:$c: ProjectData • 0x118fc:$d: DESCrypto • 0x444b2:$d: DESCrypto • 0x192c8:$e: KeepAlive
0000000E.00000002.1087171564.00000000040 B4000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xdc117:$x1: NanoCore.ClientPluginHost • 0x10ece7:$x1: NanoCore.ClientPluginHost • 0x1418a7:$x1: NanoCore.ClientPluginHost • 0xdc154:$x2: IClientNetworkHost • 0x10ed24:$x2: IClientNetworkHost • 0x1418e4:$x2: IClientNetworkHost • 0xdfc87:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x112857:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x145417:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.1087171564.00000000040 B4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 29 entries				

Unpacked PEs

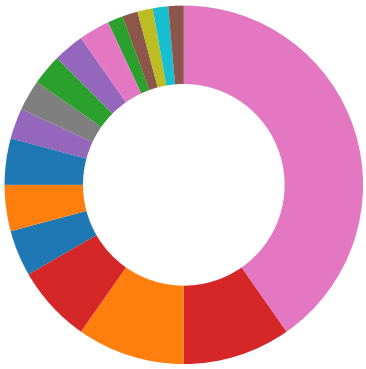
Source	Rule	Description	Author	Strings
19.2.InstallUtil.exe.4e10000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
19.2.InstallUtil.exe.4e10000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
19.2.InstallUtil.exe.5040000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
19.2.InstallUtil.exe.5040000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
19.2.InstallUtil.exe.5040000.6.raw.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
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

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)

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:

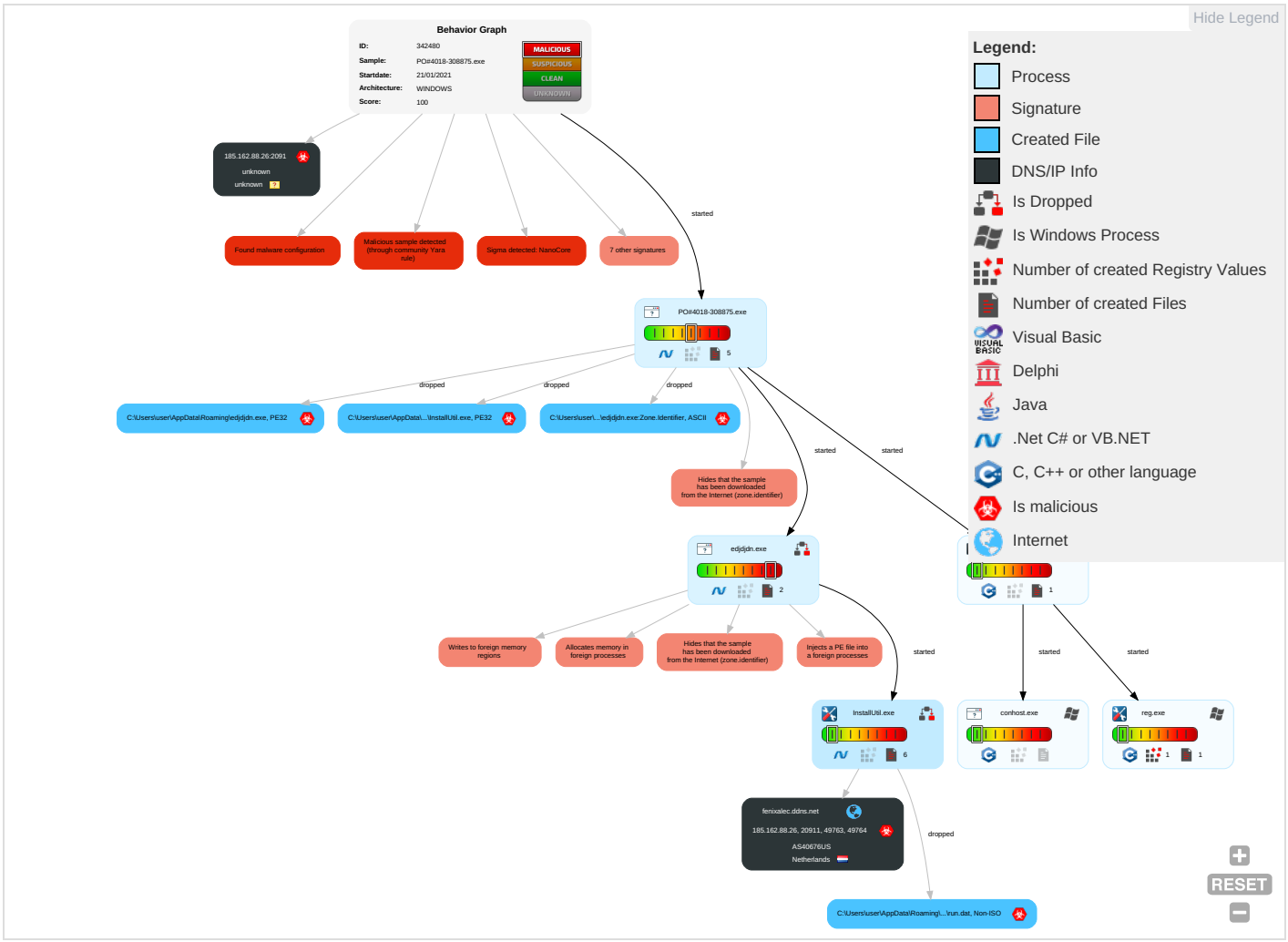
Detected Nanocore Rat

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	Masquerading 1	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encr Char
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non- Port
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	Rem Softw
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- Appli Laye Proto
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	Appli Laye Proto
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	Multi Com
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	Com Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Deobfuscate/Decode Files or Information 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)	Hidden Files and Directories 1	/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)	Obfuscated Files or Information 1	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	Software Packing 1 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

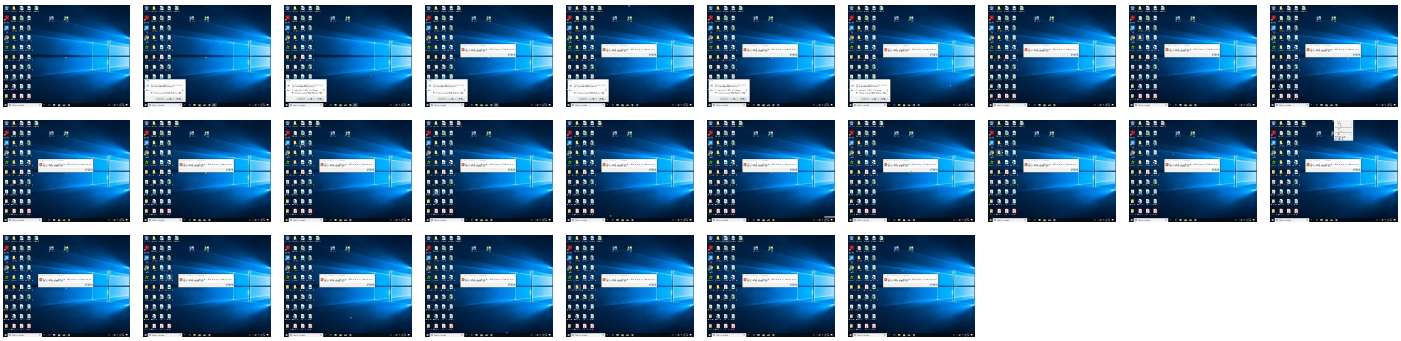
Behavior Graph

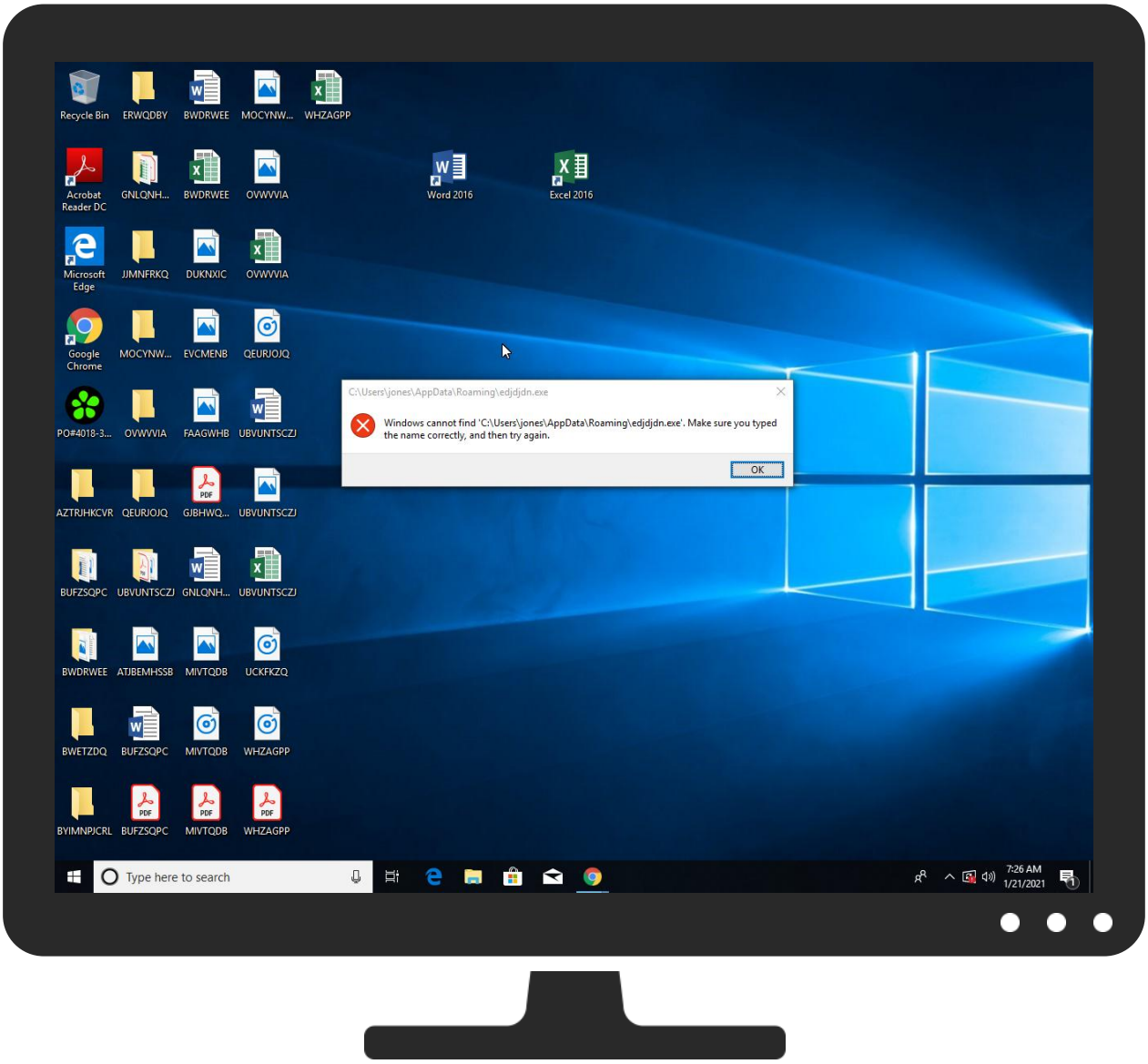


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.InstallUtil.exe.420000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.InstallUtil.exe.5040000.6.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/IdentB	0%	Avira URL Cloud	safe	
http://crl.micros:	0%	Avira URL Cloud	safe	
http://iptc.tc4xmp	0%	Avira URL Cloud	safe	

Domains and IPs

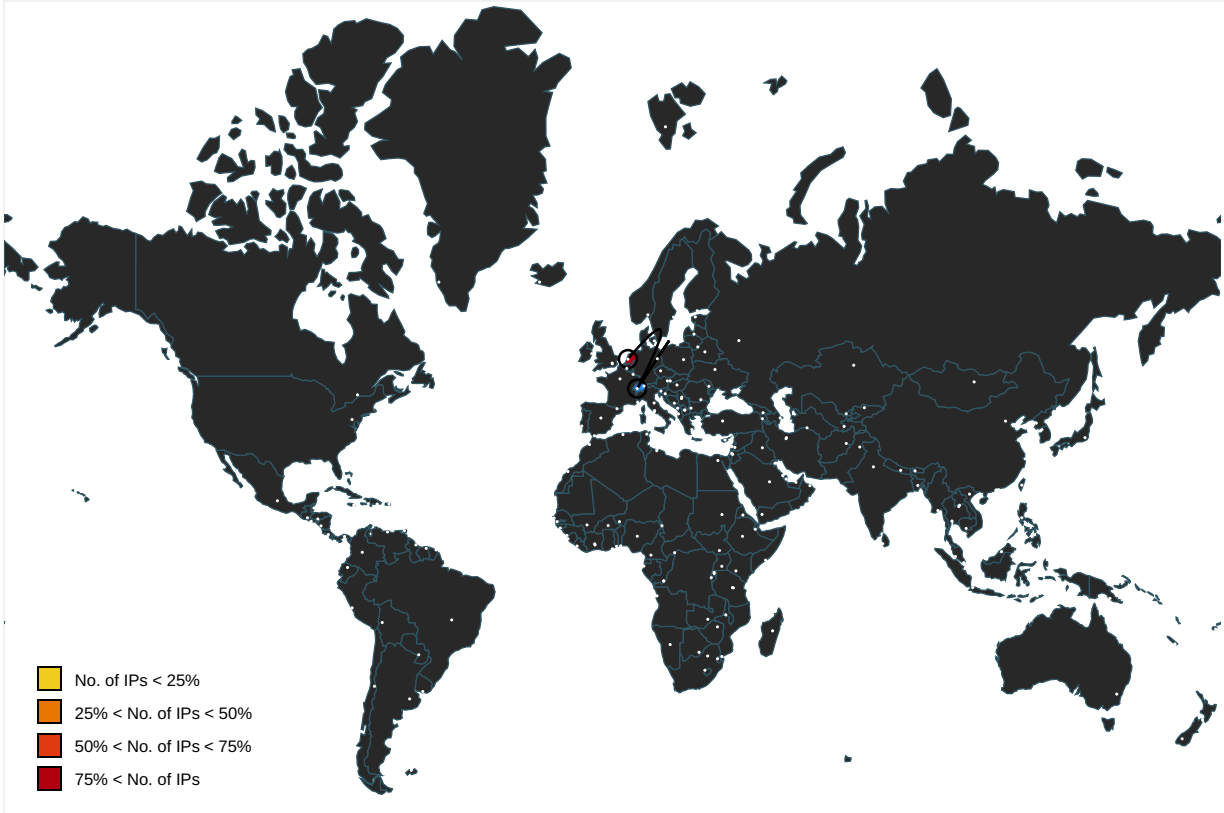
Contacted Domains

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.ado/IdentB	PO#4018-308875.exe, 00000000.00000002.781552925.000000001699000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micros:	PO#4018-308875.exe, 00000000.00000002.781295935.000000001578000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.tc4xmp	edjdjdn.exe, 0000000E.00000002.1079742606.0000000000BA9000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342480
Start date:	21.01.2021
Start time:	07:22:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#4018-308875.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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@10/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 0.7%) • Quality average: 38.6% • Quality standard deviation: 35.1%
HCA Information:	• Successful, ratio: 98% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 51.104.139.180, 92.122.213.247, 92.122.213.194, 205.185.216.10, 205.185.216.42, 52.155.217.156, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.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
07:23:44	API Interceptor	197x Sleep call for process: PO#4018-308875.exe modified
07:23:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vsg63637 C:\Users\user\AppData\Roaming\edjddn.exe
07:23:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vsg63637 C:\Users\user\AppData\Roaming\edjdjdn.exe
07:24:31	API Interceptor	227x Sleep call for process: edjdjdn.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.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.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.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Ulma9B5jo1.exe	Get hash	malicious	Browse	• 104.149.57.92
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Request for Quotation.exe	Get hash	malicious	Browse	• 45.34.249.53
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	t1XJOlYvhExZyrm.exe	Get hash	malicious	Browse	• 104.225.208.15
	SWIFT_COPY00993Payment_advic4555pdf.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 104.149.57.92
	SWIFT-COPY Payment advice3243343.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	NPD76122.exe	Get hash	malicious	Browse	• 104.217.23 1.247
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	d2mISAbTQN.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	n41pVXkYCe.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 104.217.23 1.248

JA3 Fingerprints

No context

Dropped Files

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	74725794.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.exe.log	
Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895EABB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• 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: Mi9eI6wu1p.exe, Detection: malicious, Browse • Filename: OJ4zX7G77Y.exe, Detection: malicious, Browse • Filename: IMG_50781.pdf.exe, Detection: malicious, Browse • Filename: IMG_25579.pdf.exe, Detection: malicious, Browse • Filename: IMG_40317.pdf.exe, Detection: malicious, Browse • Filename: PO#4018-308875.pdf.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.8504.exe, Detection: malicious, Browse • Filename: IMG_80137.pdf.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: MEDUSI492126.pdf.exe, Detection: malicious, Browse • Filename: 2GNCGUZ6JU.exe, Detection: malicious, Browse • Filename: IMG_53771.pdf.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.fb5363e0cae04979.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: silkOrder00110.pdf.exe, Detection: malicious, Browse • Filename: 74725794.exe, Detection: malicious, Browse • Filename: 74725794.exe, Detection: malicious, Browse
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:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:J1dt:7v
MD5:	69FC7A084233A9D318566A39B29761DF
SHA1:	9DB017FBFB8901731C39F8C483067A0AF47F8184
SHA-256:	B1E5088ECDFA706C9D85DA82363C2B27FAB16992FF6EFE2094762B9A0297B66D
SHA-512:	8F6F36DB75F7C84A6C8BE57E1F255F3BD6816046FC2DE9DEDFC1B25A593894DCD8024C6FF059389C1C51D45677C6B65E2276B6968C0585CFBC67717652BF527
Malicious:	**true**
Reputation:	low
Preview:	/..L..H

C:\Users\user\AppData\Roaming\edjdjdn.exe	
Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1103872
Entropy (8bit):	4.423145414224415
Encrypted:	false
SSDEEP:	6144:wbsFaMJcy4y50jRVCdT3/ceLDcLuZTvyH+mff7BBTkNAo23KB2pTwcSn9vCfEvgH:5hH50jwcEc6tyHpTkJ23d9ZSn9VtN
MD5:	37BB301570706E9B086C26C16E7CDB83
SHA1:	9FF8D1DCCA0C34F62113CD7F0A5028923299CD27
SHA-256:	4E599DDA2D5D0F3CAD7AC5451A39CB1C4934EA0F10FD9163E82711455AAF3EFD
SHA-512:	215F8B9165A273D12CC2BBF2F74172FFAD4D2FEF3B56B48DEDAC18B5785B12C44A358B0B701CE2099472D9A8FE20CA35686801731209DB2276DAC5D39AA864C8
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....YF\.....V..... .....@.. ....`.....W.....R..... ..... ..H.....text..... ..... ..`.rsrc....R.....T.....@..@.reloc..... .....@..B.....H.....Le..H:.....>...@/...6.....p.8(..]....._.n.(.$.4.....H..^SjA....0A-.g.I.....h".....{.....LC..;^_.5py.l'..Jf.J.1..j. q.@...o.w..A((.f...<.D'.}.).....9....!.8.....29...a...7.1.d.Q5\..s.?7.E`..N..{.^>. t....XCW..O..N.g{.H.8.....=x..,.iZEdo.p..P.NH>_..A.....*...).[.Y4$h.V...;p.Z.,."N..O..`.S.a...o.m6u.R(w.}....=.....l.G..{Y.g.B.V.....[....{..B.K.L.Jlg.8.....=:O3Il... .r..q.}n..&./.....UH..

C:\Users\user\AppData\Roaming\edjdjdn.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO#4018-308875.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
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):	4.423145414224415

General

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.exe
File size:	1103872
MD5:	37bb301570706e9b086c26c16e7cdb83
SHA1:	9ff8d1dcca0c34f62113cd7f0a5028923299cd27
SHA256:	4e599dda2d5d0f3cad7ac5451a39cb1c4934ea0f10fd9163e82711455aaf3efd
SHA512:	215f8b9165a273d12cc2bbf2f74172ffad4d2fef3b56b48dedac18b5785b12c44a358b0b701ce2099472d9a8fe20ca35686801731209db2276dac5d39aa864c8
SSDEEP:	6144:wbsFaMJcy4y50jRVCdT3/ceLDcLuZTvyH+mff7BBTkNAo23KB2pTwcSn9vCfEvgH:5hH50jwcEc6tyHpTkJ23d9ZSn9VtN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....YF\.....V..... .....@.. ....` .....

File Icon

Icon Hash:	9071d0cc686c6c00

Static PE Info

General

Entrypoint:	0x4a9fee
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:	0x5C465993 [Mon Jan 21 23:45:23 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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add al, 00h
add eax, dword ptr [eax]
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax+0000000Eh], al
pushad
add dword ptr [eax], eax
adc byte ptr [eax], 00000000h
add byte ptr [eax], al
nop
add dword ptr [eax], eax
sbb byte ptr [eax], 00000000h
add byte ptr [eax], al
rol byte ptr [ecx], 00000000h
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
or dword ptr [eax], eax
xor al, byte ptr [eax]
add byte ptr [eax], al
mov byte ptr [eax], al
add byte ptr [eax+00000033h], al
mov al, byte ptr [34800000h]
add byte ptr [eax], al
add byte ptr [eax+35800000h], bh
add byte ptr [eax], al
add al, dl
add byte ptr [eax], al
xor byte ptr [esi], 00000000h
add byte ptr [eax], al
call 00007F365C1BDE15h
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
cmp byte ptr [eax], 00000000h
add byte ptr [eax], al
sbb byte ptr [ecx], al
add byte ptr [eax+00000039h], al
xor byte ptr [ecx], al
add byte ptr [eax+0000003Ah], al
dec eax
add dword ptr [eax], eax
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
lock add dword ptr [eax], eax
add 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 [ecx], 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	0xa9f94	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0x652c6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x110000	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	0xa7ff4	0xa8000	False	0.529007684617	data	5.51964409902	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x652c6	0x65400	False	0.0656105324074	data	1.74098903041	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x110000	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	0xaa2b0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xaa718	0x810	data		
RT_ICON	0xaaf28	0x988	data		
RT_ICON	0xab8b0	0x10a8	data		
RT_ICON	0xac958	0x25a8	data		
RT_ICON	0xaef00	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 65279, next used block 4286513152		
RT_ICON	0xb3128	0x94a8	data		
RT_ICON	0xbc5d0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xccdf8	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x10ee20	0x84	data		
RT_VERSION	0x10eea4	0x238	data	English	United States
RT_MANIFEST	0x10f0dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

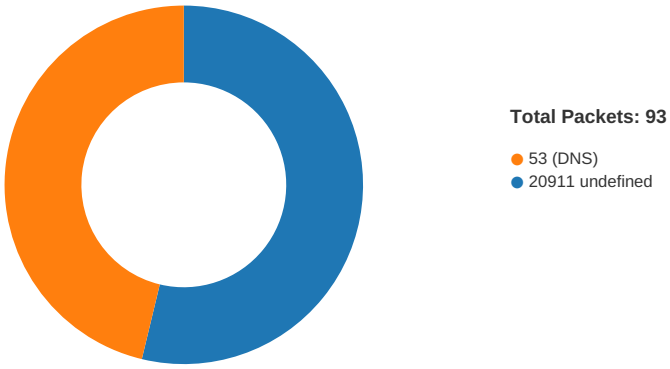
Description	Data
InternalName	ICQSetup
FileVersion	10.0.42760
ProductName	ICQSetup
ProductVersion	10.0.42760
FileDescription	ICQSetup
OriginalFilename	ICQSetup.exe
Translation	0x0009 0x04b0

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 21, 2021 07:25:10.084757090 CET	49763	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:10.135430098 CET	20911	49763	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:10.636509895 CET	49763	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:10.686858892 CET	20911	49763	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:11.199024916 CET	49763	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:11.249466896 CET	20911	49763	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:15.404979944 CET	49764	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:15.455677986 CET	20911	49764	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:15.965150118 CET	49764	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:16.016422987 CET	20911	49764	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:16.527636051 CET	49764	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:16.578141928 CET	20911	49764	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:20.607485056 CET	49765	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:20.658657074 CET	20911	49765	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:21.168693066 CET	49765	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:21.219743967 CET	20911	49765	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:21.732074022 CET	49765	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:21.783231974 CET	20911	49765	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:26.519938946 CET	49766	20911	192.168.2.4	185.162.88.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:25:26.570497990 CET	20911	49766	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:27.075679064 CET	49766	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:27.127592087 CET	20911	49766	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:27.637871981 CET	49766	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:27.688370943 CET	20911	49766	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:31.765475035 CET	49767	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:31.816122055 CET	20911	49767	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:32.325874090 CET	49767	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:32.376573086 CET	20911	49767	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:32.888333082 CET	49767	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:32.938956976 CET	20911	49767	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:37.023281097 CET	49768	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:37.073843002 CET	20911	49768	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:37.576272011 CET	49768	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:37.627008915 CET	20911	49768	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:38.138797998 CET	49768	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:38.189377069 CET	20911	49768	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:42.453793049 CET	49769	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:42.504384995 CET	20911	49769	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:43.014149904 CET	49769	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:43.064822912 CET	20911	49769	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:43.576734066 CET	49769	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:43.627396107 CET	20911	49769	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:47.641136885 CET	49770	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:47.692082882 CET	20911	49770	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:48.202152967 CET	49770	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:48.252870083 CET	20911	49770	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:48.764609098 CET	49770	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:48.815094948 CET	20911	49770	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:52.829230070 CET	49771	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:52.879786968 CET	20911	49771	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:53.390049934 CET	49771	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:53.440536022 CET	20911	49771	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:53.952632904 CET	49771	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:54.003262043 CET	20911	49771	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:58.578113079 CET	49772	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:58.628762007 CET	20911	49772	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:59.140527964 CET	49772	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:59.191127062 CET	20911	49772	185.162.88.26	192.168.2.4
Jan 21, 2021 07:25:59.703069925 CET	49772	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:25:59.753623009 CET	20911	49772	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:03.832163095 CET	49773	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:03.882600069 CET	20911	49773	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:04.390923023 CET	49773	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:04.441529036 CET	20911	49773	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:04.953460932 CET	49773	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:05.003958941 CET	20911	49773	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:09.179330111 CET	49774	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:09.229964018 CET	20911	49774	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:09.735121012 CET	49774	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:09.785792112 CET	20911	49774	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:10.297653913 CET	49774	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:10.348231077 CET	20911	49774	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:14.362057924 CET	49775	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:14.412486076 CET	20911	49775	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:14.923171997 CET	49775	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:14.974080086 CET	20911	49775	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:15.485615015 CET	49775	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:15.536632061 CET	20911	49775	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:19.668240070 CET	49776	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:19.718915939 CET	20911	49776	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:20.236001015 CET	49776	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:20.286365986 CET	20911	49776	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:20.800519943 CET	49776	20911	192.168.2.4	185.162.88.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:26:20.851195097 CET	20911	49776	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:25.040997028 CET	49777	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:25.091607094 CET	20911	49777	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:25.595813990 CET	49777	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:25.646759033 CET	20911	49777	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:26.158415079 CET	49777	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:26.209120035 CET	20911	49777	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:32.531191111 CET	49778	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:32.581801891 CET	20911	49778	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:33.097881079 CET	49778	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:33.148626089 CET	20911	49778	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:33.659120083 CET	49778	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:33.709517002 CET	20911	49778	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:37.784584045 CET	49779	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:37.835364103 CET	20911	49779	185.162.88.26	192.168.2.4
Jan 21, 2021 07:26:38.346894026 CET	49779	20911	192.168.2.4	185.162.88.26
Jan 21, 2021 07:26:38.397449970 CET	20911	49779	185.162.88.26	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:23:43.614543915 CET	49257	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:43.665257931 CET	53	49257	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:44.689234018 CET	62389	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:44.739881039 CET	53	62389	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:45.495834112 CET	49910	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:45.551877975 CET	53	49910	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:46.378259897 CET	55854	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:46.426289082 CET	53	55854	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:47.343100071 CET	64549	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:47.399133921 CET	53	64549	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:48.887177944 CET	63153	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:48.935190916 CET	53	63153	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:51.199719906 CET	52991	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:51.255995989 CET	53	52991	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:52.165663958 CET	53700	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:52.221847057 CET	53	53700	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:52.642466068 CET	51726	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:52.690581083 CET	53	51726	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:53.182290077 CET	56794	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:53.240659952 CET	53	56794	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:54.135055065 CET	56534	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:55.134255886 CET	56534	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:56.140866041 CET	56534	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:56.191446066 CET	53	56534	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:57.023505926 CET	56627	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:57.074285030 CET	53	56627	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:57.981590033 CET	56621	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:58.032367945 CET	53	56621	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:58.942996025 CET	63116	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:58.990801096 CET	53	63116	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:59.904337883 CET	64078	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:59.926062107 CET	64801	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:23:59.955013037 CET	53	64078	8.8.8.8	192.168.2.4
Jan 21, 2021 07:23:59.983828068 CET	53	64801	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:13.170032978 CET	61721	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:13.217726946 CET	53	61721	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:15.464132071 CET	51255	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:15.523135900 CET	53	51255	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:16.321850061 CET	61522	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:16.372677088 CET	53	61522	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:17.001885891 CET	52337	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:17.049832106 CET	53	52337	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:17.496665955 CET	55046	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 07:24:17.544656038 CET	53	55046	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:17.828429937 CET	49612	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:17.892405987 CET	53	49612	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:18.001795053 CET	49285	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:18.049751043 CET	53	49285	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:18.627716064 CET	50601	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:18.686820984 CET	53	50601	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:19.556876898 CET	60875	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:19.616302013 CET	53	60875	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:20.426493883 CET	56448	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:20.475693941 CET	53	56448	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:21.379967928 CET	59172	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:21.430691004 CET	53	59172	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:22.010098934 CET	62420	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:22.059067011 CET	53	62420	8.8.8.8	192.168.2.4
Jan 21, 2021 07:24:33.951409101 CET	60579	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:24:34.009349108 CET	53	60579	8.8.8.8	192.168.2.4
Jan 21, 2021 07:25:04.093010902 CET	50183	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:25:04.140887976 CET	53	50183	8.8.8.8	192.168.2.4
Jan 21, 2021 07:25:06.455203056 CET	61531	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:25:06.522239923 CET	53	61531	8.8.8.8	192.168.2.4
Jan 21, 2021 07:25:26.455594063 CET	49228	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:25:26.516936064 CET	53	49228	8.8.8.8	192.168.2.4
Jan 21, 2021 07:25:31.706206083 CET	59794	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:25:31.764043093 CET	53	59794	8.8.8.8	192.168.2.4
Jan 21, 2021 07:25:36.960380077 CET	55916	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:25:37.016804934 CET	53	55916	8.8.8.8	192.168.2.4
Jan 21, 2021 07:25:58.479531050 CET	52752	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:25:58.540647030 CET	53	52752	8.8.8.8	192.168.2.4
Jan 21, 2021 07:26:03.769551039 CET	60542	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:26:03.828701973 CET	53	60542	8.8.8.8	192.168.2.4
Jan 21, 2021 07:26:09.121685028 CET	60689	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:26:09.177673101 CET	53	60689	8.8.8.8	192.168.2.4
Jan 21, 2021 07:26:31.458743095 CET	64206	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:26:32.472063065 CET	64206	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:26:32.529617071 CET	53	64206	8.8.8.8	192.168.2.4
Jan 21, 2021 07:26:37.726634979 CET	50904	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:26:37.783082008 CET	53	50904	8.8.8.8	192.168.2.4
Jan 21, 2021 07:26:42.976655006 CET	57525	53	192.168.2.4	8.8.8.8
Jan 21, 2021 07:26:43.034219980 CET	53	57525	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2021 07:25:26.455594063 CET	192.168.2.4	8.8.8.8	0xd9e8	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:25:31.706206083 CET	192.168.2.4	8.8.8.8	0xc317	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:25:36.960380077 CET	192.168.2.4	8.8.8.8	0x2c98	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:25:58.479531050 CET	192.168.2.4	8.8.8.8	0x8a06	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:03.769551039 CET	192.168.2.4	8.8.8.8	0x854f	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:09.121685028 CET	192.168.2.4	8.8.8.8	0xe025	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:31.458743095 CET	192.168.2.4	8.8.8.8	0x21b9	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:32.472063065 CET	192.168.2.4	8.8.8.8	0x21b9	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:37.726634979 CET	192.168.2.4	8.8.8.8	0x368b	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:42.976655006 CET	192.168.2.4	8.8.8.8	0x9362	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

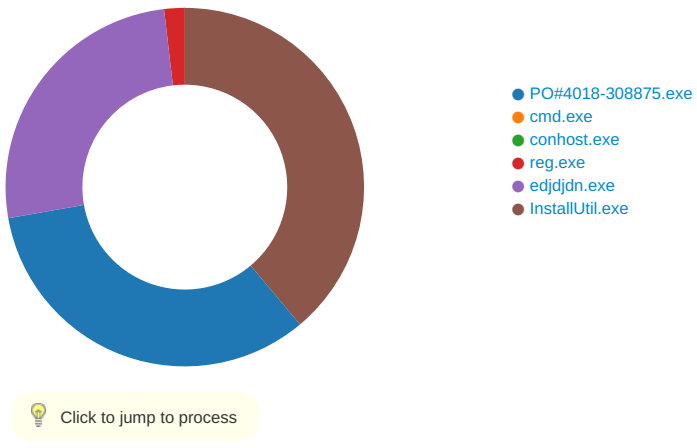
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 07:25:26.516936064 CET	8.8.8.8	192.168.2.4	0xd9e8	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:25:31.764043093 CET	8.8.8.8	192.168.2.4	0xc317	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:25:37.016804934 CET	8.8.8.8	192.168.2.4	0x2c98	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:25:58.540647030 CET	8.8.8.8	192.168.2.4	0x8a06	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:03.828701973 CET	8.8.8.8	192.168.2.4	0x854f	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:09.177673101 CET	8.8.8.8	192.168.2.4	0xe025	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:32.529617071 CET	8.8.8.8	192.168.2.4	0x21b9	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:37.783082008 CET	8.8.8.8	192.168.2.4	0x368b	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 21, 2021 07:26:43.034219980 CET	8.8.8.8	192.168.2.4	0x9362	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO#4018-308875.exe PID: 4780 Parent PID: 6048

General

Start time:	07:23:37
Start date:	21/01/2021

Path:	C:\Users\user\Desktop\PO#4018-308875.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO#4018-308875.exe'
Imagebase:	0xd10000
File size:	1103872 bytes
MD5 hash:	37BB301570706E9B086C26C16E7CDB83
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: 00000000.00000002.782898982.0000000004AC7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.782898982.0000000004AC7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.782898982.0000000004AC7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.783786131.0000000004C5D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.783786131.0000000004C5D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.783786131.0000000004C5D000.00000004.00000001.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	59FE8AB	CopyFileExW
C:\Users\user\AppData\Roaming\edjdjdn.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	59FE8AB	CopyFileExW
C:\Users\user\AppData\Roaming\edjdjdn.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	59FE8AB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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 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	59FE8AB	CopyFileExW
C:\Users\user\AppData\Roaming\edjdjdn.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 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 93 59 46 5c 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 80 0a 00 00 56 06 00 00 00 00 00 00 ee 9f 0a 00 00 20 00 00 00 a0 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 11 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....YF\.......... ....V........... ....@.. ....`.................	success or wait	5	59FE8AB	CopyFileExW
C:\Users\user\AppData\Roaming\edjdjdn.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	59FE8AB	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#4018-308875.exe.log	unknown	1451	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"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=	success or wait	1	6D6EC907	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D3103DE	ReadFile

Analysis Process: cmd.exe PID: 3220 Parent PID: 4780

General

Start time:	07:23:42
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'vsg63637' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\edjdjdn.exe'
Imagebase:	0x11d0000
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: 1440 Parent PID: 3220

General

Start time:	07:23:43
Start date:	21/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5760 Parent PID: 3220

General

Start time:	07:23:43
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'vsg63637' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\edjdjdn.exe'
Imagebase:	0x940000
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	vsg63637	unicode	C:\Users\user\AppData\Roaming\edjdjdn.exe	success or wait	1	945A1D	RegSetValueExW

Analysis Process: edjdjdn.exe PID: 2016 Parent PID: 4780

General

Start time:	07:24:26
Start date:	21/01/2021
Path:	C:\Users\user\AppData\Roaming\edjdjdn.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\edjdjdn.exe'
Imagebase:	0x340000
File size:	1103872 bytes
MD5 hash:	37BB301570706E9B086C26C16E7CDB83
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: 0000000E.00000002.1087650939.000000000424A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.1087650939.000000000424A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.1087650939.000000000424A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.1087171564.00000000040B4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.1087171564.00000000040B4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.1087171564.00000000040B4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.1086961721.0000000004021000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.1086961721.0000000004021000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.1086961721.0000000004021000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	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	6D3DCF06	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown

Analysis Process: InstallUtil.exe PID: 5480 Parent PID: 2016

General

Start time:	07:25:02
Start date:	21/01/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x50000
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: 00000013.00000002.1086796443.0000000004E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.1086796443.0000000004E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.1082965333.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.1082965333.00000000035A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.1078429432.0000000000422000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.1078429432.0000000000422000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.1078429432.0000000000422000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.1087119513.0000000005040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.1087119513.0000000005040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.1087119513.0000000005040000.00000004.00000001.sdmp, Author: Joe Security
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	6D3DCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D3DCF06	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	6C22BEFF	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	6C221E60	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	6C22BEFF	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	6C22BEFF	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	2f f7 90 4c d5 bd d8 48	/..L...H	success or wait	1	6C221B4F	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	512	success or wait	1	6D39D72F	unknown

Disassembly

Code Analysis