ID: 341430
Sample Name:
MEDUSI492126.pdf.exe
Cookbook: default.jbs
Time: 10:46:05
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

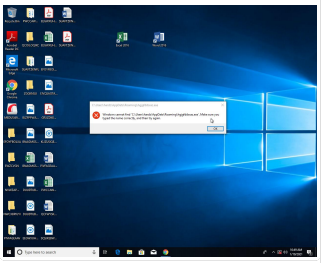
Analysis Report MEDUSI492126.pdf.exe

Overview

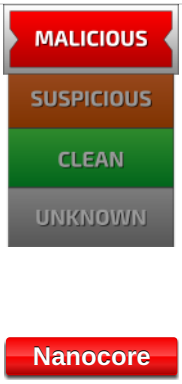
General Information

Sample Name:	MEDUSI492126.pdf.exe
Analysis ID:	341430
MD5:	3f350480fd99bd2..
SHA1:	7fda4a5e9610d3d.
SHA256:	c914e1cead39ffb..
Tags:	exe MSC NanoCore RAT

Most interesting Screenshot:



Detection

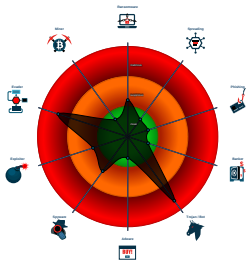


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- MEDUSI492126.pdf.exe (PID: 6088 cmdline: 'C:\Users\user\Desktop\MEDUSI492126.pdf.exe' MD5: 3F350480FD99BD2E9C9B32C9FA1BF4E0)
  - cmd.exe (PID: 4764 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'retyujik' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 4280 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'retyujik' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - hgjgfddsxaz.exe (PID: 6920 cmdline: 'C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe' MD5: 3F350480FD99BD2E9C9B32C9FA1BF4E0)
    - InstallUtil.exe (PID: 5896 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
00000014.00000002.592972004.000000000417 2000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4342d:$x1: NanoCore.ClientPluginHost • 0x4346a:$x2: IClientNetworkHost • 0x46f9d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000014.00000002.592972004.000000000417 2000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000014.00000002.592972004.000000000417 2000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x43195:$a: NanoCore • 0x431a5:$a: NanoCore • 0x433d9:$a: NanoCore • 0x433ed:$a: NanoCore • 0x4342d:$a: NanoCore • 0x431f4:$b: ClientPlugin • 0x433f6:$b: ClientPlugin • 0x43436:$b: ClientPlugin • 0x4331b:$c: ProjectData • 0x43d22:$d: DESCrypto • 0x4b6ee:$e: KeepAlive • 0x496dc:$g: LogClientMessage • 0x458d7:$i: get_Connected • 0x44058:$j: #=q • 0x44088:$j: #=q • 0x440a4:$j: #=q • 0x440d4:$j: #=q • 0x440f0:$j: #=q • 0x4410c:$j: #=q • 0x4413c:$j: #=q • 0x44158:$j: #=q
00000000.00000002.338088857.0000000004A4 A000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x11007:$x1: NanoCore.ClientPluginHost • 0x43bc5:$x1: NanoCore.ClientPluginHost • 0x11044:$x2: IClientNetworkHost • 0x43c02:$x2: IClientNetworkHost • 0x14b77:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x47735:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.338088857.0000000004A4 A000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.InstallUtil.exe.58e0000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
24.2.InstallUtil.exe.58e0000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
24.2.InstallUtil.exe.5900000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
24.2.InstallUtil.exe.5900000.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
24.2.InstallUtil.exe.5900000.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 7 entries				

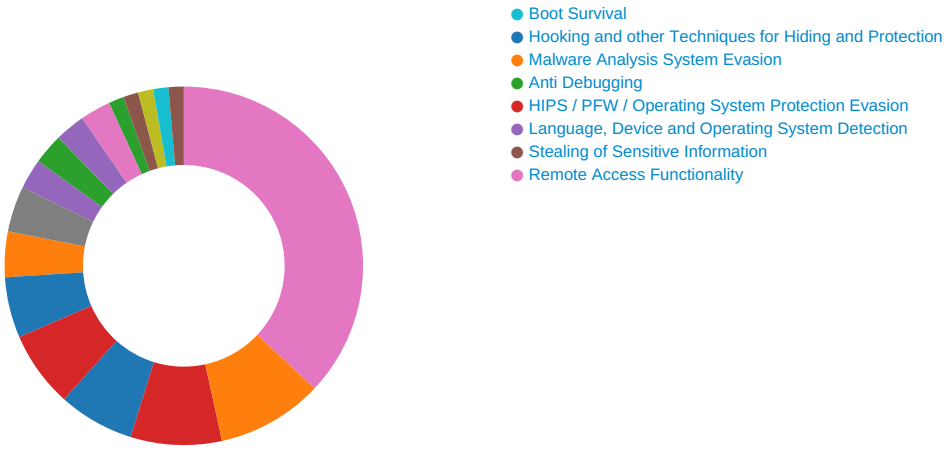
Sigma Overview

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)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

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:

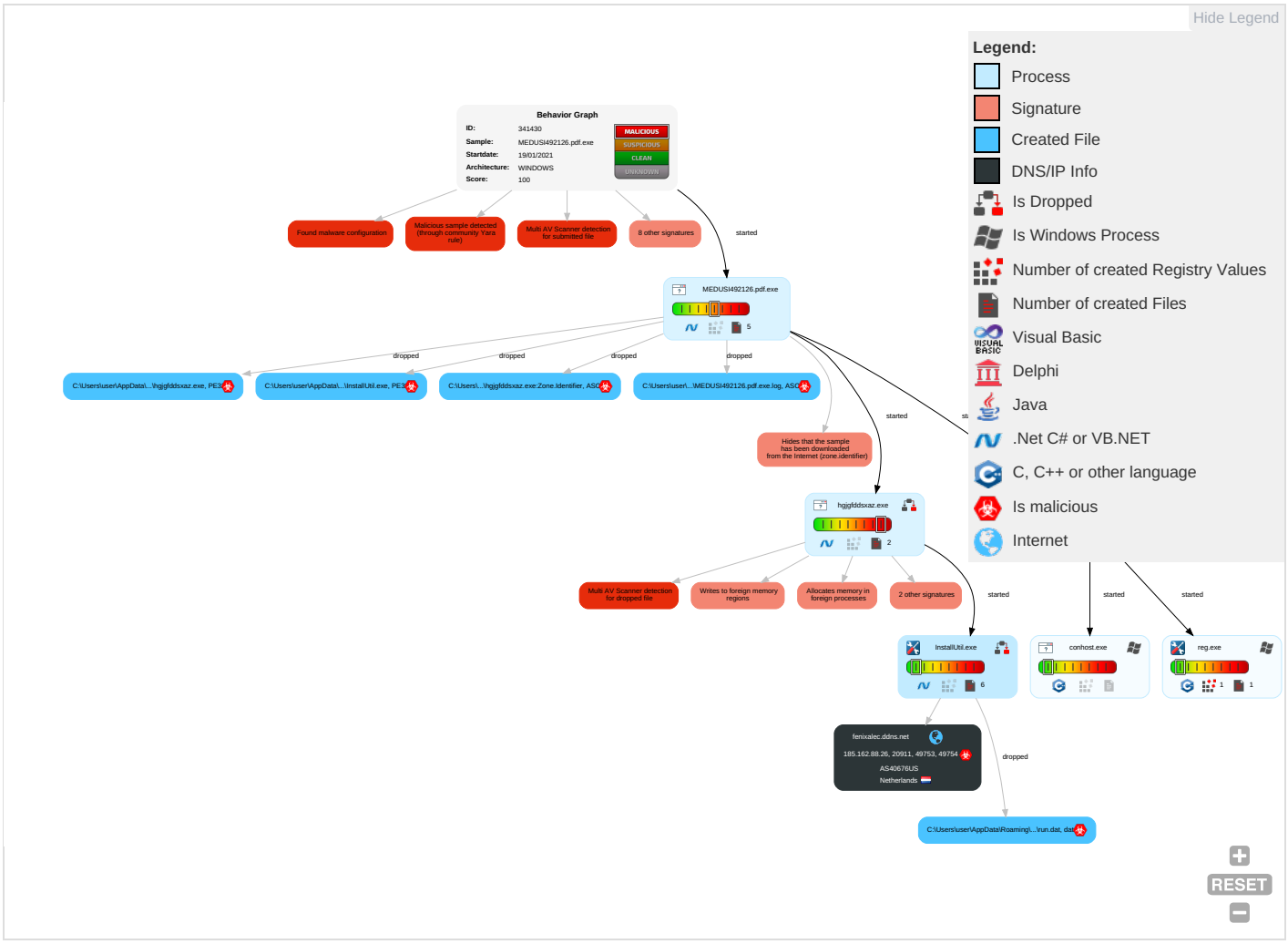
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Eff
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Masquerading 1 1	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Modify Registry 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SI Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Ro Ba

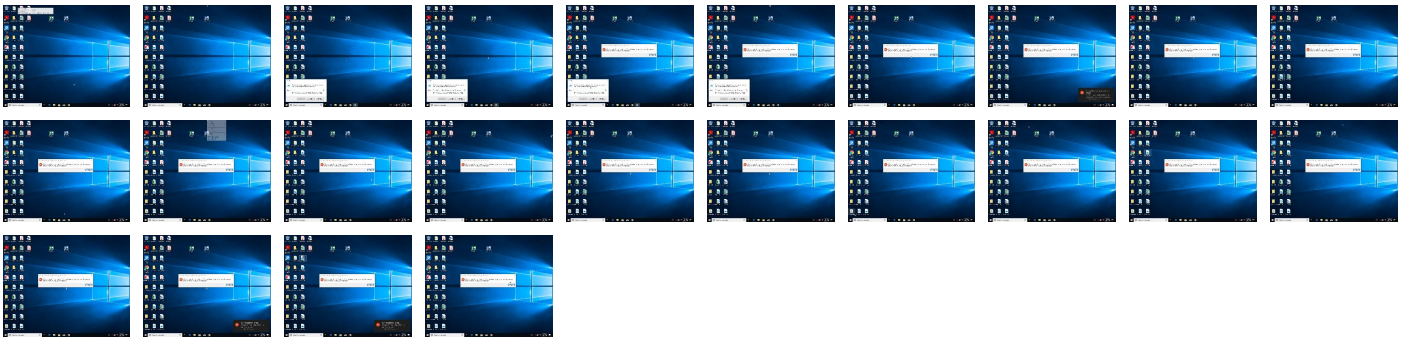
Behavior Graph

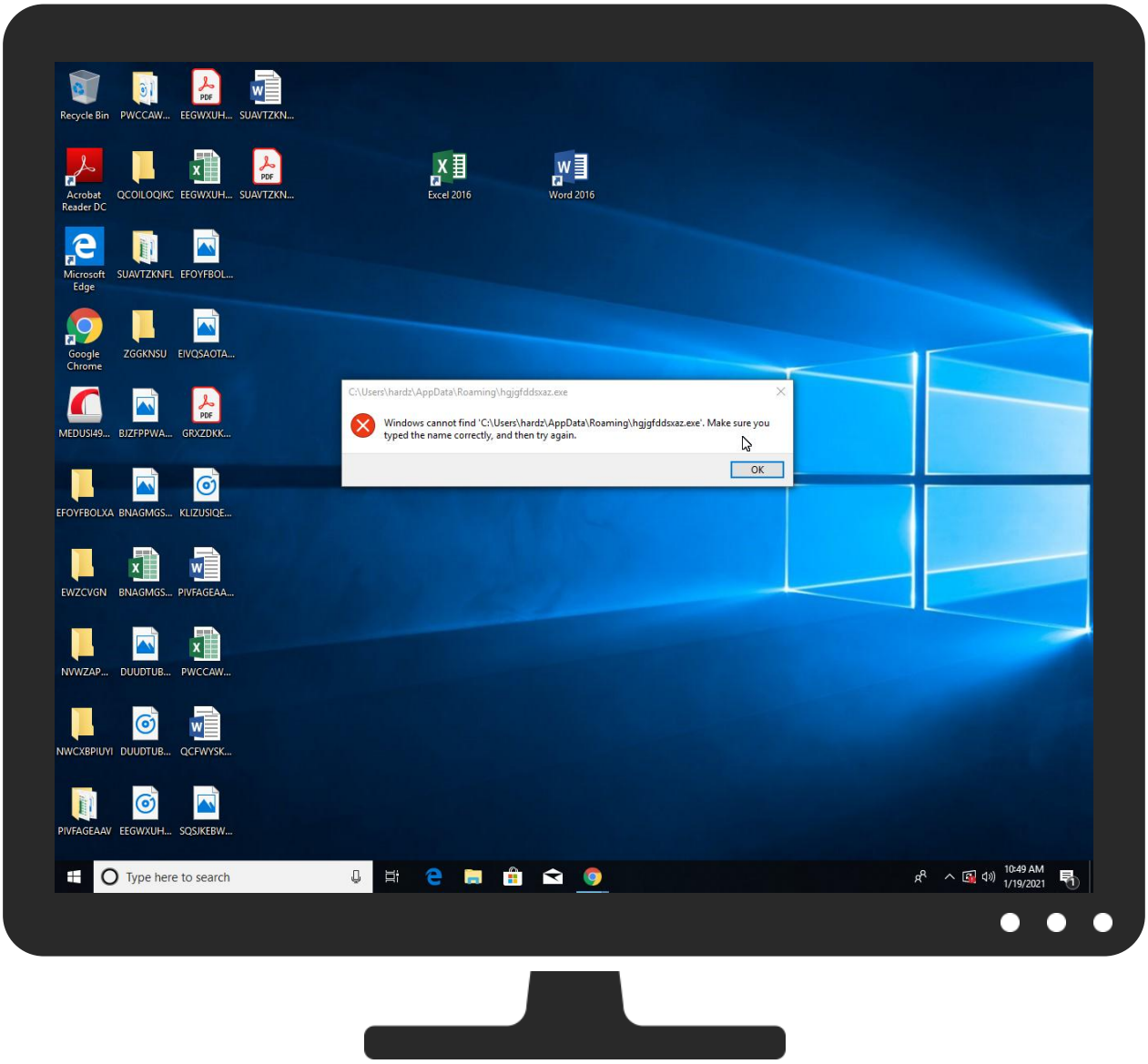


Screenshots

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
MEDUSI492126.pdf.exe	34%	Virustotal		Browse
MEDUSI492126.pdf.exe	20%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe	34%	Virustotal		Browse
C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe	20%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.InstallUtil.exe.5900000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
24.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		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	MEDUSI492126.pdf.exe, 00000000.00000003.335533082.0000000001849000.00000004.00000001.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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341430
Start date:	19.01.2021
Start time:	10:46:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MEDUSI492126.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:	33
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@6/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 53.1% • Quality standard deviation: 34.8%
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 • Exclude process from analysis (whitelisted): 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): 52.255.188.83, 40.88.32.150, 23.210.248.85, 51.11.168.160, 92.122.213.194, 92.122.213.247, 93.184.221.240, 51.103.5.186, 52.254.96.93, 20.54.26.129, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, wu.azureedge.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.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
10:47:07	API Interceptor	199x Sleep call for process: MEDUSI492126.pdf.exe modified
10:47:08	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run retyujik C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe
10:47:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run retyujik C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe
10:48:00	API Interceptor	217x Sleep call for process: hgjgfddsxaz.exe modified

Joe Sandbox View / Context

IPs

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

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fenixalec.ddns.net	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	Request for Quotation.exe	Get hash	malicious	Browse	• 45.34.249.53
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	t1XJOlYvhExZyrm.exe	Get hash	malicious	Browse	• 104.225.208.15
	SWIFT_COPY00993Payment_advic4555pdf.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 104.149.57.92
	SWIFT-COPY Payment advice3243343.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	NPD76122.exe	Get hash	malicious	Browse	• 104.217.23 1.247
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	d2mISAbTQN.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	n41pVXkYCe.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	53McmgaUJP.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	BsR85tOyjL.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 173.224.209.14
	athwlp3L1t.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	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_13791.pdf.exe	Get hash	malicious	Browse	
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	
	pls.exe	Get hash	malicious	Browse	
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.505.30555.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MEDUSI492126.pdf.exe.log

Process:	C:\Users\user\Desktop\MEDUSI492126.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:MLU84qpE4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6nx1qE4j:Mgv2HKXeHKlEHU0YHKhQnouHIW7HKjxm
MD5:	A3A3A85F33BFAD9A069110C913DAD818
SHA1:	E2DA64F657CC1DE2DD27787B9F365CF84508E833
SHA-256:	DE24C0B69909C9864E60CC7DA755471426C0CDF549ECDBBE65E31F2359633555
SHA-512:	3A553007132E1050A97A262A21DCA3AB1A3442EBB51E6DDD7337B6454A97472937ADE6FDEB52568A30D32EAEF01800A4BC16C7F75236E9E2001C975D8C514F1
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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, Cul

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

Process:	C:\Users\user\Desktop\MEDUSI492126.pdf.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• 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 • Filename: Order_BC012356.pdf.exe, Detection: malicious, Browse • Filename: pls.exe, Detection: malicious, Browse • Filename: Document#20014464370.pdf.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.505.30555.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
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:FP:N
MD5:	0F9353C664ED8948D75EC8D08B5C87EA
SHA1:	25646DB26539BB0EB26344950033CFA1A794555A
SHA-256:	4E078D6CA2C68B2A23D8795BFB3B48E7D8A63675A1CE72FF7F60C205192438D8
SHA-512:	DD430C5E05196BD0D0F5BB31BC8722E8F78440727E5E579A7788BB1A66F66F0AD3420F29C542D72D09D59D7FA97ECB903622335CF1981B05C7BE45949DEFA43
Malicious:	**true**
Reputation:	low
Preview:	\.....H

C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe	
Process:	C:\Users\user\Desktop\MEDUSI492126.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	942080
Entropy (8bit):	5.3133493633744555
Encrypted:	false
SSDEEP:	6144:gGg4kMF2VtDYY4ULce5ly3DF/5892Rfx7y7H+mff7BBTkNAo23KB2pTwcSn9vCfK:gkkzjLzlyzF/B1aHpTkJ23d9ZSn9Vtz
MD5:	3F350480FD99BD2E9C9B32C9FA1BF4E0
SHA1:	7FDA4A5E9610D3DF93EC08C855E73A4B2B0570F4
SHA-256:	C914E1CEAD39FFB086BB87029BCEA3673F8159087EF8CD7C1CF49ECEBA97EE07
SHA-512:	CA55F5A74EE282E988654B01C500AA93CA51BBEF415255E1C850739C603B00F777A86B13935C56EFCAEF0850E623EACB2C3EA29773897CD88146E16C4C26A3D
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....K..... .....@.. ....`.....P...K.....|..... ..... ..H.....text..... ..... ..`.rsrc....|.....~.....@..@.reloc..... .....^.....@..B.....H.....4%.....%...h.....O^."b..o._g.F.3.$..2PU#.....5l.`.....@.R9.P...?..]!&.....N.o.J.Mx.....l. .o9....*..&.. ...^.d.|.X..z4...x.....[.o...8.e.g...a....V#V.a@..k....Z7NB.#.....L....h.....exl>7..{..{.(....#ii.>.}.v".!-YC.=..e.:tc._.e..|ey...bL....T.K..pKnT..Qr.w...b..6..5..W..w1..U...j.o.....^..E.!.B.. l....Z.....iT...Fu3.=.).d.u.G.....<G..H..YY...}E.>....,..A.W.%.i..>T.....

C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\MEDUSI492126.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):	5.3133493633744555
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:	MEDUSI492126.pdf.exe
File size:	942080
MD5:	3f350480fd99bd2e9c9b32c9fa1bf4e0
SHA1:	7fda4a5e9610d3df93ec08c855e73a4b2b0570f4
SHA256:	c914e1cead39ffb086bb87029bcea3673f8159087ef8cd7c1cf49eceba97ee07
SHA512:	ca55f5a74ee282e988654b01c500aa93ca51bbef415255e1c850739c603b00f777a86b13935c56efcaef0850e623eacb2c3ea29773897cd88146e16c4c26a3d9
SSDEEP:	6144:gGg4kMF2VtDYY4ULce5ly3DF/5892Rfx7y7H+mff7BBTkNAo23KB2pTwcSn9vCfK:gkkzjLzlyzF/B1aHpTkJ23d9ZSn9Vtz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....K..... .....@.. ..... `.....

File Icon

Icon Hash:	98bee6a283829ec2

Static PE Info

General

Entrypoint:	0x4dfc9e
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:	0x7E64BFF [Thu Mar 14 22:47:27 1974 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdfc50	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x7ca6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	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	0xddca4	0xdde00	False	0.442184198944	data	5.26895380135	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x7ca6	0x7e00	False	0.37394593254	data	5.76833442238	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	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	0xe0340	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0xe0468	0x1e8	data		
RT_ICON	0xe0650	0x2e8	data		
RT_ICON	0xe0938	0x668	dBase IV DBT of `.DBF, block length 1536, next free block index 40, next free block 224, next used block 768		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe0fa0	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xe1508	0x6c8	data		
RT_ICON	0xe1bd0	0x8a8	data		
RT_ICON	0xe2478	0xea8	data		
RT_ICON	0xe3320	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xe3788	0x988	data		
RT_ICON	0xe4110	0x10a8	data		
RT_ICON	0xe51b8	0x25a8	data		
RT_GROUP_ICON	0xe7760	0xae	data		
RT_VERSION	0xe7810	0x2ac	data	English	United States
RT_MANIFEST	0xe7abc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

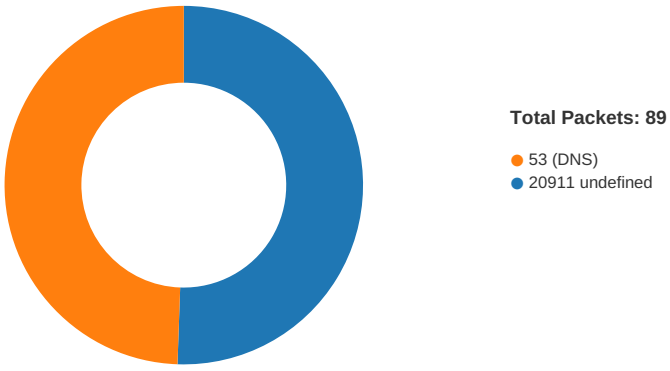
Description	Data
LegalCopyright	Copyright Opera Software 2020
InternalName	Opera
FileVersion	72.0.3815.400
CompanyName	Opera Software
ProductName	Opera Installer
ProductVersion	72.0.3815.400
FileDescription	Opera Installer
Translation	0x0409 0x04b0

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 19, 2021 10:48:39.799494028 CET	49753	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:39.850183010 CET	20911	49753	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:40.352771997 CET	49753	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:40.403362989 CET	20911	49753	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:40.915400982 CET	49753	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:40.965732098 CET	20911	49753	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:45.026196003 CET	49754	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:45.077275038 CET	20911	49754	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:45.587601900 CET	49754	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:45.638434887 CET	20911	49754	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:46.150259018 CET	49754	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:46.201178074 CET	20911	49754	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:50.254041910 CET	49755	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:50.304646015 CET	20911	49755	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:50.806936026 CET	49755	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:50.857517004 CET	20911	49755	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:51.369324923 CET	49755	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:51.419913054 CET	20911	49755	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:57.271637917 CET	49756	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:57.322338104 CET	20911	49756	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:57.822993040 CET	49756	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:57.873528004 CET	20911	49756	185.162.88.26	192.168.2.3
Jan 19, 2021 10:48:58.385634899 CET	49756	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:48:58.436278105 CET	20911	49756	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:02.513295889 CET	49757	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:02.563802004 CET	20911	49757	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:03.073507071 CET	49757	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:03.124948025 CET	20911	49757	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:03.636002064 CET	49757	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:03.686744928 CET	20911	49757	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:07.763022900 CET	49758	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:07.813810110 CET	20911	49758	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:08.323844910 CET	49758	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:08.374386072 CET	20911	49758	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:08.886410952 CET	49758	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:08.936927080 CET	20911	49758	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:12.951097012 CET	49759	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:13.001657963 CET	20911	49759	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:13.511966944 CET	49759	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:13.562710047 CET	20911	49759	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:14.074307919 CET	49759	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:14.124994040 CET	20911	49759	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:18.298017979 CET	49760	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:18.349931955 CET	20911	49760	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:18.855928898 CET	49760	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:18.906542063 CET	20911	49760	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:19.418483973 CET	49760	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:19.469137907 CET	20911	49760	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:23.483203888 CET	49761	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:23.533657074 CET	20911	49761	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:24.043881893 CET	49761	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:24.094469070 CET	20911	49761	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:24.606532097 CET	49761	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:24.657203913 CET	20911	49761	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:29.104944944 CET	49762	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:29.155567884 CET	20911	49762	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:29.669359922 CET	49762	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:29.719840050 CET	20911	49762	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:30.231869936 CET	49762	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:30.282670975 CET	20911	49762	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:34.414669037 CET	49763	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:34.465291977 CET	20911	49763	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:34.966722012 CET	49763	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:35.017597914 CET	20911	49763	185.162.88.26	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 10:49:35.529232025 CET	49763	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:35.579931974 CET	20911	49763	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:39.664004087 CET	49764	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:39.715728998 CET	20911	49764	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:40.231916904 CET	49764	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:40.282701969 CET	20911	49764	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:40.792174101 CET	49764	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:40.842853069 CET	20911	49764	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:44.970376015 CET	49765	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:45.021239042 CET	20911	49765	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:45.526060104 CET	49765	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:45.576704025 CET	20911	49765	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:46.088587046 CET	49765	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:46.139318943 CET	20911	49765	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:50.152645111 CET	49766	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:50.204139948 CET	20911	49766	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:50.713996887 CET	49766	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:50.764695883 CET	20911	49766	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:51.276689053 CET	49766	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:51.327265024 CET	20911	49766	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:55.340390921 CET	49767	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:55.391318083 CET	20911	49767	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:55.901890039 CET	49767	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:55.953944921 CET	20911	49767	185.162.88.26	192.168.2.3
Jan 19, 2021 10:49:56.464458942 CET	49767	20911	192.168.2.3	185.162.88.26
Jan 19, 2021 10:49:56.515445948 CET	20911	49767	185.162.88.26	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 10:47:08.111047029 CET	64938	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:08.159177065 CET	53	64938	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:08.882317066 CET	60152	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:08.930907965 CET	53	60152	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:10.325284004 CET	57544	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:10.373076916 CET	53	57544	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:11.764595032 CET	55984	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:11.815249920 CET	53	55984	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:12.877542973 CET	64185	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:12.925451040 CET	53	64185	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:13.742988110 CET	65110	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:13.790821075 CET	53	65110	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:14.522783041 CET	58361	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:14.570580006 CET	53	58361	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:15.391833067 CET	63492	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:15.442576885 CET	53	63492	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:17.407469988 CET	60831	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:17.458266020 CET	53	60831	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:19.788703918 CET	60100	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:19.839462996 CET	53	60100	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:22.608747959 CET	53195	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:22.666836977 CET	53	53195	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:23.339910030 CET	50141	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:23.390599012 CET	53	50141	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:24.048716068 CET	53023	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:24.096540928 CET	53	53023	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:24.311482906 CET	49563	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:24.359246969 CET	53	49563	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:25.178965092 CET	51352	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:25.235213995 CET	53	51352	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:30.015100002 CET	59349	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:30.071324110 CET	53	59349	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:32.023372889 CET	57084	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:32.071376085 CET	53	57084	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 10:47:33.406830072 CET	58823	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:33.464437008 CET	53	58823	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:37.605518103 CET	57568	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:37.653419971 CET	53	57568	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:38.522526026 CET	50540	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:38.573723078 CET	53	50540	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:39.357963085 CET	54366	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:39.414597988 CET	53	54366	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:40.416655064 CET	53034	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:40.464510918 CET	53	53034	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:42.104981899 CET	57762	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:42.161494970 CET	53	57762	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:44.241782904 CET	55435	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:44.289643049 CET	53	55435	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:49.065593004 CET	50713	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:49.210273027 CET	53	50713	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:50.214858055 CET	56132	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:50.273946047 CET	53	56132	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:51.643054008 CET	58987	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:51.707396984 CET	53	58987	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:52.957469940 CET	56579	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:53.014153957 CET	53	56579	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:54.447529078 CET	60633	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:54.503731012 CET	53	60633	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:54.952896118 CET	61292	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:55.018655062 CET	53	61292	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:55.500391960 CET	63619	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:55.556713104 CET	53	63619	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:56.653456926 CET	64938	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:56.709825039 CET	53	64938	8.8.8.8	192.168.2.3
Jan 19, 2021 10:47:58.439755917 CET	61946	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:47:58.498681068 CET	53	61946	8.8.8.8	192.168.2.3
Jan 19, 2021 10:48:00.031099081 CET	64910	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:48:00.087548971 CET	53	64910	8.8.8.8	192.168.2.3
Jan 19, 2021 10:48:00.956382036 CET	52123	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:48:01.016108036 CET	53	52123	8.8.8.8	192.168.2.3
Jan 19, 2021 10:48:01.213134050 CET	56130	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:48:01.273766041 CET	53	56130	8.8.8.8	192.168.2.3
Jan 19, 2021 10:48:33.406441927 CET	56338	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:48:33.454292059 CET	53	56338	8.8.8.8	192.168.2.3
Jan 19, 2021 10:48:36.372833014 CET	59420	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:48:36.449378967 CET	53	59420	8.8.8.8	192.168.2.3
Jan 19, 2021 10:48:57.211781025 CET	58784	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:48:57.269583941 CET	53	58784	8.8.8.8	192.168.2.3
Jan 19, 2021 10:49:02.452044010 CET	63978	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:49:02.510519028 CET	53	63978	8.8.8.8	192.168.2.3
Jan 19, 2021 10:49:07.702106953 CET	62938	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:49:07.761039019 CET	53	62938	8.8.8.8	192.168.2.3
Jan 19, 2021 10:49:29.046714067 CET	55708	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:49:29.103327036 CET	53	55708	8.8.8.8	192.168.2.3
Jan 19, 2021 10:49:34.356945038 CET	56803	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:49:34.413094044 CET	53	56803	8.8.8.8	192.168.2.3
Jan 19, 2021 10:49:39.596544981 CET	57145	53	192.168.2.3	8.8.8.8
Jan 19, 2021 10:49:39.652793884 CET	53	57145	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 10:48:57.211781025 CET	192.168.2.3	8.8.8.8	0xf11b	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:02.452044010 CET	192.168.2.3	8.8.8.8	0x1ab3	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:07.702106953 CET	192.168.2.3	8.8.8.8	0xb9fd	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 10:49:29.046714067 CET	192.168.2.3	8.8.8.8	0x5341	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:34.356945038 CET	192.168.2.3	8.8.8.8	0x301e	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:39.596544981 CET	192.168.2.3	8.8.8.8	0x3e5b	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

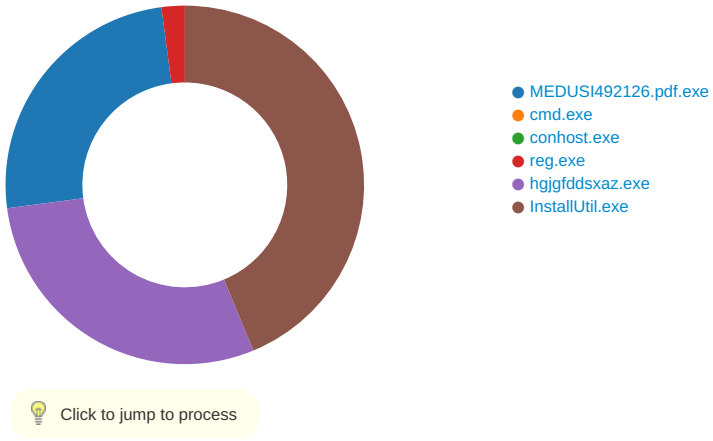
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 10:48:57.269583941 CET	8.8.8.8	192.168.2.3	0xf11b	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:02.510519028 CET	8.8.8.8	192.168.2.3	0x1ab3	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:07.761039019 CET	8.8.8.8	192.168.2.3	0xb9fd	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:29.103327036 CET	8.8.8.8	192.168.2.3	0x5341	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:34.413094044 CET	8.8.8.8	192.168.2.3	0x301e	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 19, 2021 10:49:39.652793884 CET	8.8.8.8	192.168.2.3	0x3e5b	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: MEDUSI492126.pdf.exe PID: 6088 Parent PID: 5744

General

Start time:	10:47:01
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\MEDUSI492126.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\MEDUSI492126.pdf.exe'
Imagebase:	0xbb0000
File size:	942080 bytes
MD5 hash:	3F350480FD99BD2E9C9B32C9FA1BF4E0
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: 00000000.00000002.338088857.0000000004A4A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.338088857.0000000004A4A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.338088857.0000000004A4A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.337626085.00000000048E8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.337626085.00000000048E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.337626085.00000000048E8000.00000004.00000001.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\Microsoft\CLR_v4.0_32\UsageLogs\MEDUSI492126.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	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\Microsoft\CLR_v4.0_32\UsageLogs\MEDUSI492126.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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0303DE	ReadFile

Analysis Process: cmd.exe PID: 4764 Parent PID: 6088

General

Start time:	10:47:05
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'retyujik' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe'
Imagebase:	0xbd0000
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: 5308 Parent PID: 4764

General

Start time:	10:47:06
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 4280 Parent PID: 4764

General

Start time:	10:47:06
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'retyujik' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe'
Imagebase:	0x2f0000
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	retyujik	unicode	C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe	success or wait	1	2F5A1D	RegSetValueExW

Analysis Process: hgjgfddsxaz.exe PID: 6920 Parent PID: 6088

General

Start time:	10:47:54
Start date:	19/01/2021
Path:	C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\hgjgfddsxaz.exe'
Imagebase:	0x300000
File size:	942080 bytes
MD5 hash:	3F350480FD99BD2E9C9B32C9FA1BF4E0
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: 00000014.00000002.592972004.0000000004172000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.592972004.0000000004172000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.592972004.0000000004172000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.593076062.0000000004205000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.593076062.0000000004205000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.593076062.0000000004205000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.593637409.000000000439B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.593637409.000000000439B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.593637409.000000000439B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 34%, Virustotal, Browse • Detection: 20%, 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	6E0FCF06	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	6E0FCF06	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\d d5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8 c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown

Analysis Process: InstallUtil.exe PID: 5896 Parent PID: 6920

General

Start time:	10:48:30
Start date:	19/01/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0xe00000
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: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.589229834.00000000042A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.589229834.00000000042A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.580480048.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.580480048.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.580480048.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.592742291.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.592742291.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.592779539.0000000005900000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.592779539.0000000005900000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.592779539.0000000005900000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E0FCF06	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	6E0FCF06	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	6CF4BEFF	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	6CF41E60	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	6CF4BEFF	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	6CF4BEFF	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	5c 04 d0 d4 aa bc d8 48	\.....H	success or wait	1	6CF41B4F	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	4096	success or wait	1	6E0BD72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	512	success or wait	1	6E0BD72F	unknown

Disassembly

Code Analysis