ID: 357128
Sample Name: New Order 632487 PDF.exe
Cookbook: default.jbs
Time: 08:26:02
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

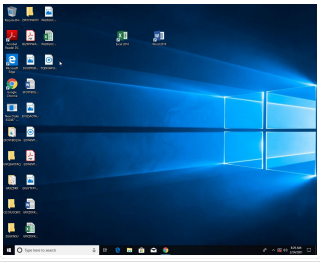
Analysis Report New Order 632487 PDF.exe

Overview

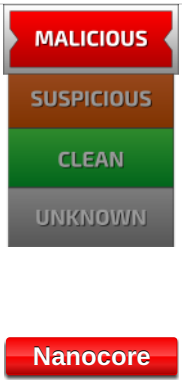
General Information

Sample Name:	New Order 632487 PDF.exe
Analysis ID:	357128
MD5:	6bb37fbe7ff7b15…
SHA1:	e0f33af458168bc..
SHA256:	2a65da255eb2ee..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection



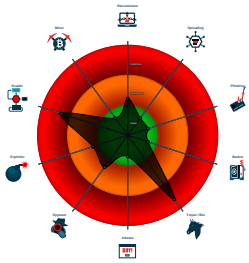
Nanocore

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

Signatures

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

Classification



Startup

- **System is w10x64**
- New Order 632487 PDF.exe (PID: 6284 cmdline: 'C:\Users\user\Desktop\New Order 632487 PDF.exe' MD5: 6BB37FBE7FF7B15C6B20A788BA9D46FF)
  - a.exe (PID: 6132 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: 6BB37FBE7FF7B15C6B20A788BA9D46FF)
- a.exe (PID: 7084 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: 6BB37FBE7FF7B15C6B20A788BA9D46FF)
  - InstallUtil.exe (PID: 6160 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- dhcpmon.exe (PID: 5440 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 6340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "d2ce8aef-f90b-4d6a-b5b0-ecbe54404c6b",
  "Group": "BOTS",
  "Domain1": "forcesbots.ddns.net",
  "Domain2": "forcesbots.ddns.net",
  "Port": 7767,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.285863508.00000000040C9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x42ed7:$x1: NanoCore.ClientPluginHost • 0x75a97:$x1: NanoCore.ClientPluginHost • 0xa8647:$x1: NanoCore.ClientPluginHost • 0x42f14:$x2: IClientNetworkHost • 0x75ad4:$x2: IClientNetworkHost • 0xa8684:$x2: IClientNetworkHost • 0x46a47:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x79607:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xac1b7:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.285863508.00000000040C9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.285863508.00000000040C9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x42c3f:$a: NanoCore • 0x42c4f:$a: NanoCore • 0x42e83:$a: NanoCore • 0x42e97:$a: NanoCore • 0x42ed7:$a: NanoCore • 0x757ff:$a: NanoCore • 0x7580f:$a: NanoCore • 0x75a43:$a: NanoCore • 0x75a57:$a: NanoCore • 0x75a97:$a: NanoCore • 0xa83af:$a: NanoCore • 0xa83bf:$a: NanoCore • 0xa85f3:$a: NanoCore • 0xa8607:$a: NanoCore • 0xa8647:$a: NanoCore • 0x42c9e:$b: ClientPlugin • 0x42ea0:$b: ClientPlugin • 0x42ee0:$b: ClientPlugin • 0x7585e:$b: ClientPlugin • 0x75a60:$b: ClientPlugin • 0x75aa0:$b: ClientPlugin
00000009.00000002.499062665.000000000396 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.499062665.000000000396 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2ef5:$a: NanoCore • 0x2f4e:$a: NanoCore • 0x2f8b:$a: NanoCore • 0x3004:$a: NanoCore • 0x166af:$a: NanoCore • 0x166c4:$a: NanoCore • 0x166f9:$a: NanoCore • 0x2f17b:$a: NanoCore • 0x2f190:$a: NanoCore • 0x2f1c5:$a: NanoCore • 0x2f57:$b: ClientPlugin • 0x2f94:$b: ClientPlugin • 0x3892:$b: ClientPlugin • 0x389f:$b: ClientPlugin • 0x1646b:$b: ClientPlugin • 0x16486:$b: ClientPlugin • 0x164b6:$b: ClientPlugin • 0x166cd:$b: ClientPlugin • 0x16702:$b: ClientPlugin • 0x2ef37:$b: ClientPlugin • 0x2ef52:$b: ClientPlugin
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.InstallUtil.exe.5290000.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
9.2.InstallUtil.exe.5290000.10.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
9.2.InstallUtil.exe.5290000.10.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.New Order 632487 PDF.exe.41f97a8.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.New Order 632487 PDF.exe.41f97a8.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 107 entries				

Sigma Overview

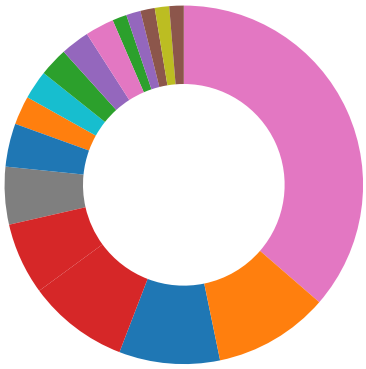
System Summary:

Sigma detected: NanoCore

Signature Overview

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

Remote Access Functionality



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- 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)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

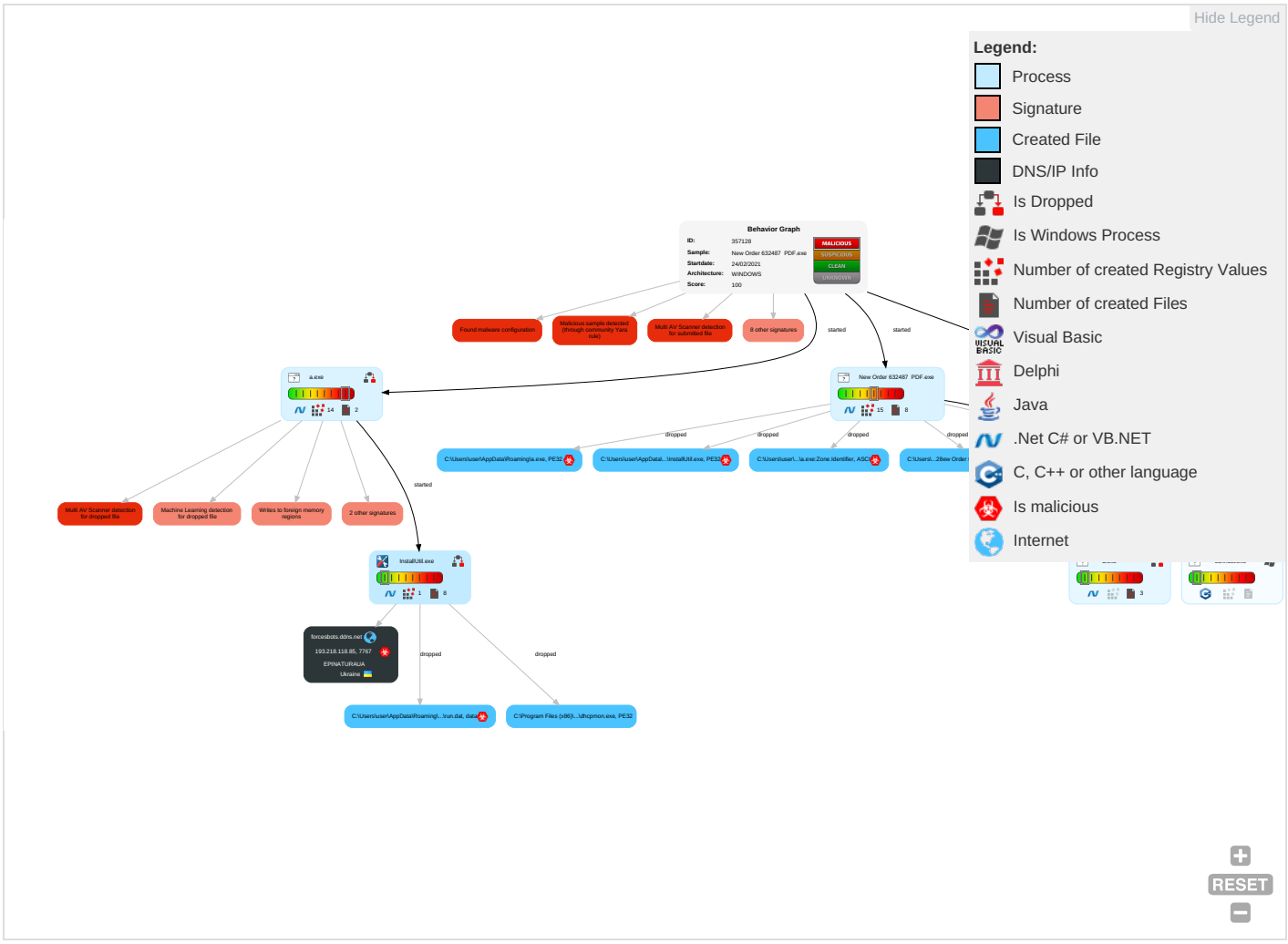
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Scheduled Task/Job	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-S Port 1
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remot Softwa
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	Software Packing 1 3	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 4	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 4	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

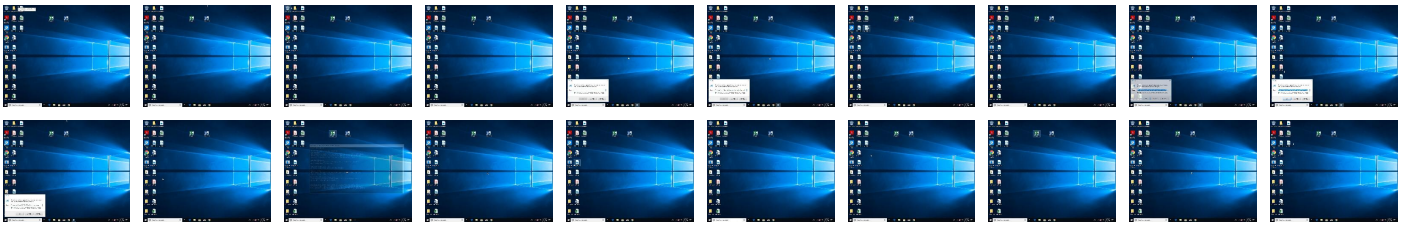
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
New Order 632487 PDF.exe	43%	Virustotal		Browse
New Order 632487 PDF.exe	22%	Metadefender		Browse
New Order 632487 PDF.exe	83%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
New Order 632487 PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\a.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
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\a.exe	22%	Metadefender		Browse
C:\Users\user\AppData\Roaming\a.exe	83%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.InstallUtil.exe.5290000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
forcesbots.ddns.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ns.adb	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
forcesbots.ddns.net	2%	Virustotal		Browse
forcesbots.ddns.net	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
forcesbots.ddns.net	193.218.118.85	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

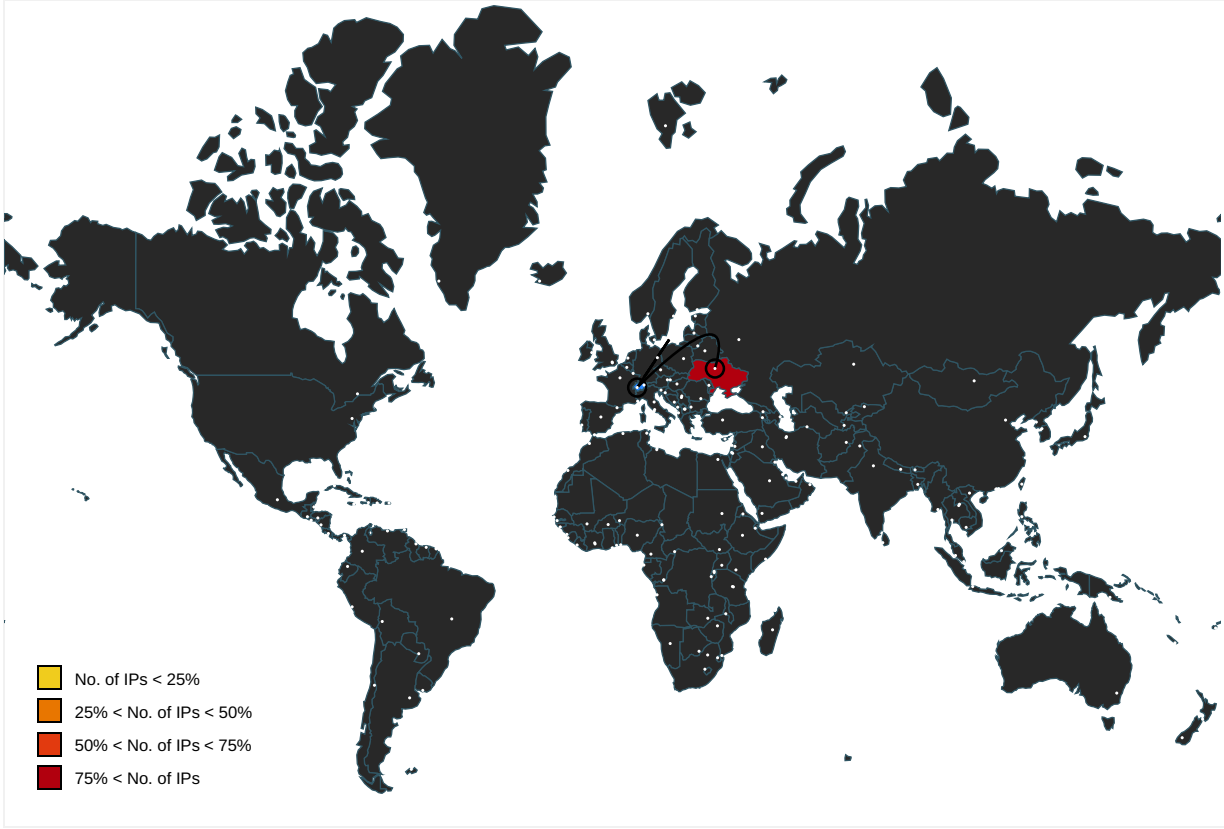
Name	Malicious	Antivirus Detection	Reputation
forcesbots.ddns.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adb	New Order 632487 PDF.exe, 00000000.00000003.224354770.00000000008982000.00000004.00000001.sdmp, a.exe, 00000006.00000003.266327505.0000000008A72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr2/GTS1O1.crt0	a.exe, 00000007.00000002.28688 2790.0000000002CEE000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	New Order 632487 PDF.exe, 000 00000.00000003.232281575.00000 00008982000.00000004.00000001. sdmp, New Order 632487 PDF.exe, 00000000.00000003.279683656 .0000000008989000.00000004.000 00001.sdmp, a.exe, 00000006.00 000003.269005618.0000000008A72 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	New Order 632487 PDF.exe, 000 00000.00000003.232281575.00000 00008982000.00000004.00000001. sdmp, New Order 632487 PDF.exe, 00000000.00000003.279683656 .0000000008989000.00000004.000 00001.sdmp, a.exe, 00000006.00 000003.269005618.0000000008A72 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/PraneethMadush	a.exe	false		high
http://ocsp.pki.goog/gts1o1core0	a.exe, 00000007.00000002.28688 2790.0000000002CEE000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	New Order 632487 PDF.exe, 000 00000.00000002.283313795.00000 000027A1000.00000004.00000001. sdmp, a.exe, 00000006.00000002 .492451984.0000000002701000.00 000004.00000001.sdmp, a.exe, 0 0000007.00000002.286813086.000 0000002CC1000.00000004.0000000 1.sdmp	false		high
http://schema.org/WebPage	New Order 632487 PDF.exe, 000 00000.00000002.283382208.00000 000027CD000.00000004.00000001. sdmp, a.exe, 00000006.00000002 .492633026.000000000272D000.00 000004.00000001.sdmp, a.exe, 0 0000006.00000002.492720693.000 0000002743000.00000004.0000000 1.sdmp, a.exe, 00000007.000000 02.286925043.0000000002D04000. 00000004.00000001.sdmp, a.exe, 00000007.00000002.286882790.0 000000002CEE000.00000004.00000 001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	a.exe, 00000007.00000002.28688 2790.0000000002CEE000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	New Order 632487 PDF.exe, 000 00000.00000003.232281575.00000 00008982000.00000004.00000001. sdmp, New Order 632487 PDF.exe, 00000000.00000003.279683656 .0000000008989000.00000004.000 00001.sdmp, a.exe, 00000006.00 000003.269005618.0000000008A72 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.218.118.85	unknown	Ukraine		207656	EPINATURAUA	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357128
Start date:	24.02.2021
Start time:	08:26:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order 632487 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:	29
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@8/10@6/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.6%) • Quality average: 39.7% • Quality standard deviation: 34.5%
HCA Information:	• Successful, ratio: 99% • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 51.104.144.132, 204.79.197.200, 13.107.21.200, 93.184.220.29, 92.122.145.220, 104.42.151.234, 142.250.185.164, 13.64.90.137, 13.88.21.125, 168.61.161.212, 52.147.198.201, 23.218.208.56, 52.255.188.83, 8.248.147.254, 8.253.207.121, 67.26.83.254, 8.248.119.254, 8.253.207.120, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many 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
08:27:09	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk
08:27:26	API Interceptor	1x Sleep call for process: New Order 632487 PDF.exe modified
08:27:28	API Interceptor	1x Sleep call for process: a.exe modified
08:27:37	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.218.118.85	docs-034.exe	Get hash	malicious	Browse	
	p9W7XrJg7B.exe	Get hash	malicious	Browse	
	wqxfQkYM.exe	Get hash	malicious	Browse	
	Y2EnkSyG.exe	Get hash	malicious	Browse	
	068vjTbZ.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
forcesbots.ddns.net	New Order 863127 PDF.exe	Get hash	malicious	Browse	• 197.210.84.206

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EPINATURAUA	docs-034.exe	Get hash	malicious	Browse	• 193.218.118.85
	hse8DRMQnI.exe	Get hash	malicious	Browse	• 193.218.118.125
	FickerStealer.exe	Get hash	malicious	Browse	• 193.218.118.167
	p9W7XrJg7B.exe	Get hash	malicious	Browse	• 193.218.118.85
	wqxfQkYM.exe	Get hash	malicious	Browse	• 193.218.118.85
	Y2EnkSyG.exe	Get hash	malicious	Browse	• 193.218.118.85
	068vjTbZ.exe	Get hash	malicious	Browse	• 193.218.118.85
	docs090.exe	Get hash	malicious	Browse	• 193.218.118.190
	belgelervk.exe	Get hash	malicious	Browse	• 193.218.118.190
	docs-06.exe	Get hash	malicious	Browse	• 193.218.118.190
	docs094.exe	Get hash	malicious	Browse	• 193.218.118.190
	q7Q5SdJy.exe	Get hash	malicious	Browse	• 193.218.118.190

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASERAL FERDAN.exe	Get hash	malicious	Browse	
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASERAL FERDAN.exe	Get hash	malicious	Browse	
	REQUEST FOR OFFER.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	v2.exe	Get hash	malicious	Browse	
	MPO-003234.exe	Get hash	malicious	Browse	
	Payment copy.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42841.18110.exe	Get hash	malicious	Browse	
	DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe	Get hash	malicious	Browse	
	index_2021-02-18-20_41.exe	Get hash	malicious	Browse	
	XXXXXXXXXXXXX.exe	Get hash	malicious	Browse	
	IMG_144907.exe	Get hash	malicious	Browse	
	VIIIIIIIIIIIIC.exe	Get hash	malicious	Browse	
	lQN1zlLSGa.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Sorted Properties.exe	Get hash	malicious	Browse	
	DB_DHL_AWB_00117390021_AD03990399003920032.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	
	REQUEST FOR OFFER.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	v2.exe	Get hash	malicious	Browse	
	MPO-003234.exe	Get hash	malicious	Browse	
	Payment copy.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42841.18110.exe	Get hash	malicious	Browse	
	DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe	Get hash	malicious	Browse	
	index_2021-02-18-20_41.exe	Get hash	malicious	Browse	
	XXXXXXXXXXXXXX.exe	Get hash	malicious	Browse	
	IMG_144907.exe	Get hash	malicious	Browse	
	VIIIIIIIIIIIIC.exe	Get hash	malicious	Browse	
	lQN1zlLSGa.exe	Get hash	malicious	Browse	
	Sorted Properties.exe	Get hash	malicious	Browse	
	DB_DHL_AWB_00117390021_AD03990399003920032.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe, Detection: malicious, Browse • Filename: HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe, Detection: malicious, Browse • Filename: REQUEST FOR OFFER.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: v2.exe, Detection: malicious, Browse • Filename: MPO-003234.exe, Detection: malicious, Browse • Filename: Payment copy.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: YKRAB010B_KHE_Preminary Packing List.xlsx.exe, Detection: malicious, Browse • Filename: RTM DIAS - CTM.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Artemis249E62CF9BAE.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Packed2.42841.18110.exe, Detection: malicious, Browse • Filename: DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe, Detection: malicious, Browse • Filename: index_2021-02-18-20_41.exe, Detection: malicious, Browse • Filename: XXXXXXXXXXXXXX.exe, Detection: malicious, Browse • Filename: IMG_144907.exe, Detection: malicious, Browse • Filename: VIIIIIIIIIIIIC.exe, Detection: malicious, Browse • Filename: lQN1zlLSGa.exe, Detection: malicious, Browse • Filename: Sorted Properties.exe, Detection: malicious, Browse • Filename: DB_DHL_AWB_00117390021_AD03990399003920032.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Program Files (x86)\DHCP Monitor\dhcpmon.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\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order 632487 PDF.exe.log	
Process:	C:\Users\user\Desktop\New Order 632487 PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1128
Entropy (8bit):	5.3642098150017015
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHH
MD5:	F559E0C1EE1946CCFCDFC8B1AAF4790D
SHA1:	C64B80AF0CFE0C5116442D76D3B14FE76200492C
SHA-256:	CCB1CB8024F68A95F371EAF0DC9AACC53CFB4793B3201E3A288329CB22D58E48
SHA-512:	5A70156D95C609AFCCAF48EA552E45F9AC2F6A5C46F965D9E21CFBCB87F9D716A35B59B7FE0AC39D67DFCBD1E6CA75A1B6494A10150DAD86FD2BF9F66CAC/ 904
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, Publi cKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration .ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	
Process:	C:\Users\user\AppData\Roaming\a.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1128
Entropy (8bit):	5.3642098150017015
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHH
MD5:	F559E0C1EE1946CCFCDFC8B1AAF4790D
SHA1:	C64B80AF0CFE0C5116442D76D3B14FE76200492C
SHA-256:	CCB1CB8024F68A95F371EAF0DC9AACC53CFB4793B3201E3A288329CB22D58E48
SHA-512:	5A70156D95C609AFCCAF48EA552E45F9AC2F6A5C46F965D9E21CFBCB87F9D716A35B59B7FE0AC39D67DFCBD1E6CA75A1B6494A10150DAD86FD2BF9F66CAC/ 904
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, Publi cKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration .ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	950
Entropy (8bit):	5.350971482944737
Encrypted:	false
SSDEEP:	24:MLiKNE4qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MeIH2HKXwYHKhQnoPtHoxHhAHKzva
MD5:	CEE81B7EB08EE82CFE49E47B81B50D1A
SHA1:	4746C7068BD50E3309BFFDBE8983B8F27D834DFD
SHA-256:	B9A90255691E7C9D3CCBD27D00FC514DDD6087446D8DB03335CEF1B5634CC460
SHA-512:	AF5865439412974FCB6B11E22CFFF1ACA0BEBF83CF398D6056CEEF93720AF0FBCB579858C39E6AA0D989680F2180F2CA181D7D12887604B420D0E1976B8AEA7
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, 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,"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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\New Order 632487 PDF.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe, Detection: malicious, Browse • Filename: HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe, Detection: malicious, Browse • Filename: REQUEST FOR OFFER.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: v2.exe, Detection: malicious, Browse • Filename: MPO-003234.exe, Detection: malicious, Browse • Filename: Payment copy.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: YKRAB010B_KHE_Preminary Packing List.xlsx.exe, Detection: malicious, Browse • Filename: RTM DIAS - CTM.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Artemis249E62CF9BAE.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Packed2.42841.18110.exe, Detection: malicious, Browse • Filename: DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe, Detection: malicious, Browse • Filename: index_2021-02-18-20_41.exe, Detection: malicious, Browse • Filename: XXXXXXXXXXXXX.exe, Detection: malicious, Browse • Filename: IMG_144907.exe, Detection: malicious, Browse • Filename: VIIIIIIIIIIIIC.exe, Detection: malicious, Browse • Filename: lQN1zlLSGa.exe, Detection: malicious, Browse • Filename: Sorted Properties.exe, Detection: malicious, Browse • Filename: DB_DHL_AWB_00117390021_AD03990399003920032.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. .....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.reloc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....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):	2.75
Encrypted:	false
SSDEEP:	3:79P:5P
MD5:	C7477DA9F3F97638516A2477F2CC2B8B
SHA1:	9768234F199909AC29AAC801D149DA06E9076F69
SHA-256:	DF7A7D39217AD8CF412C8DF9A4D8CC0B18648CBE482BCEACE96A551C232E696E
SHA-512:	40E891484BABD402200F9F185B4C6A762A67916FBD5076E3BBC3DC8A68BF6EAF775561477307D4714E228DF4A5805F637EA2F7B5465CCBDCD26839538B272A8E
Malicious:	**true**
Preview:	k.....H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk	
Process:	C:\Users\user\Desktop\New Order 632487 PDF.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk	
Size (bytes):	854
Entropy (8bit):	3.03156476699929
Encrypted:	false
SSDEEP:	12:8wl0RsXou41w/tz0/CSLmz3qMJkHgTCNfBT/v4t2Y+xIBjK:8if4eWL0t+Vpd7aB
MD5:	C43C60D569FA0C256C556082126497D4
SHA1:	A3206A53ECCC894E6F1F7037ECB395A91EDEFF54
SHA-256:	E9F08DB61FE3C57BF38D637B3601487358AE827DC032B03F37CDA9F8551AF7F6
SHA-512:	96C92F6EE08F1578E06231B9024DEF96BD55A14190CFA824DA4A408E62B94BF6D408C73657886993302CE902C3D3C264C386B1C6D27F682B290B0E21567B7DE8
Malicious:	false
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....h.a.r.d.z.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....P.2..... ....a.exe.<.....a...e.x.e.....\....\....\....\....\a...e.x.e.$.C.:\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.a...e.x.e.....y.....>.e.L.: ..er.=y.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Roaming\a.exe	
Process:	C:\Users\user\Desktop\New Order 632487 PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	830976
Entropy (8bit):	7.301089079716191
Encrypted:	false
SSDEEP:	12288:0hGT/f7DSvWN1JuigLYVlaf+dhKeVnVBAzzP3V7B+AciC8+WrWwYgI7:/zHSvi7AYaf+dk+gzDF7Btd6fgI7
MD5:	6BB37FBE7FF7B15C6B20A788BA9D46FF
SHA1:	E0F33AF458168BCCF87FA98638192626C1053CCF
SHA-256:	2A65DA255EB2EE6CE3C4F2A9CE64E9A48491325BB44BD0FDA7C95B6A5DB64A41
SHA-512:	FFEFE12D0822DA046A06343D51DD6AE9E005E506916EC02A237E411ECD1DC7CC4A76DBC61AC1CC4F063BC9CBEB1FB54B823C73EE0049B2ADE49B4333EC2D605
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....H^.....".."...P..... .....@.. ....`.....I...O.....Z..... ..... ..H.....text..... ..... ..`.rsrc...Z.....@..@.reloc..... .....@..B.....H.....U...k.....H....|.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*Z.....o6.....*&..(7....*j..{....(...+}..... {....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*...{.....,+.....,rq..ps<...z..|....(...+*...{.....,+.....,rq..ps<...z..|....(...+*...{.....,+.....,rq..ps<...z..|....(...+*&.....*".....*Vs)...(B...t... .....*..(C...*6.(D....(....*&.{....+.*".}....*&.{....+.*

C:\Users\user\AppData\Roaming\a.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\New Order 632487 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**
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2017
Entropy (8bit):	4.663189584482275
Encrypted:	false
SSDEEP:	48:zK4Qu4D4ql0+1AcJRy0EJP64gFljVlWo3ggxUnQK2qmBvgw1+5:zKJDEcTytNe3Wo3uQVBIe+5
MD5:	9C305D95E7DA8FCA9651F7F426BB25BC
SHA1:	FDB5C18C26CF5B83EF5DC297C0F9CEBEF6A97FFC
SHA-256:	444F71CF504D22F0EE88024D61501D3B79AE5D1AFD521E72499F325F6B0B82BE
SHA-512:	F2829518AE0F6DD35C1DE1175FC8BE3E52EDCAFAD0B2455AC593F5E5D4BD480B014F52C3AE24E742B914685513BE5DF862373E75C45BB7908C775D7E2E404D3

\Device\ConDrv	
Malicious:	false
Preview:	Microsoft (R) .NET Framework Installation utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Usage: InstallUtil [/u | /uninstall] [option [...]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs them. Unlike other..options, /u applies to all assemblies, regardless of where it..appears on the command line.....Installation is done in a transactioned way: If one of the..assemblies fails to install, the installations of all other..assemblies are rolled back. Uninstall is not transactioned.....Options take the form /switch=[value]. Any option that occurs..before the name of an assembly will apply to that assembly's..installation. Options are cumulative but overridable - options..specified for one assembly will apply to the next as well unless..the option is specified with a new value. The default for

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.301089079716191
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:	New Order 632487 PDF.exe
File size:	830976
MD5:	6bb37fbe7ff7b15c6b20a788ba9d46ff
SHA1:	e0f33af458168bccf87fa98638192626c1053ccf
SHA256:	2a65da255eb2ee6ce3c4f2a9ce64e9a48491325bb44bd0da7c95b6a5db64a41
SHA512:	ffefe12d0822da046a06343d51dd6ae9e005e506916ec02a237e411ecd1dc7cc4a76dbc61ac1cc4f063bc9cbeb1fb54b823c73ee0049b2ade49b4333ec2d8605
SSDEEP:	12288:0hGT/f7DSvWN1JuigLYVlaf+dhKeVnVBAzzP3V7B+AciC8+WrWwYgI7:/zHSvi7AYaf+dk+gzDF7Btd6fgI7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....H^....."...P..... .....@.. ....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cc1be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E48BFF2 [Sun Feb 16 04:07:14 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcc16c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x65a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	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	0xca1c4	0xca200	False	0.795109094774	data	7.31108517286	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x65a	0x800	False	0.3623046875	data	3.75438294081	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.0940979256627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xce0a0	0x3d0	data		
RT_MANIFEST	0xce470	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

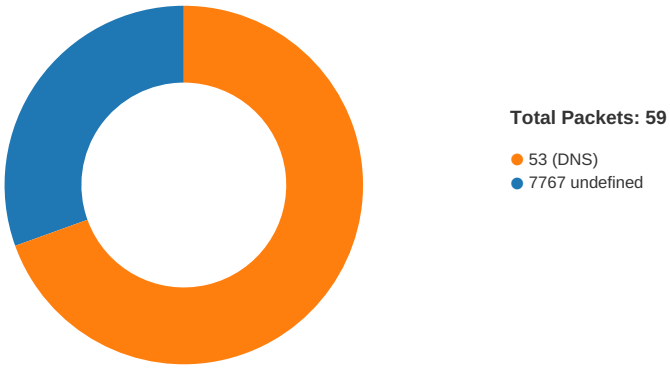
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2002 :5G3:@;<;EHBGF;9?II
Assembly Version	1.0.0.0
InternalName	New Order 632487 PDF.exe
FileVersion	4.7.9.11
CompanyName	:5G3:@;<;EHBGF;9?II
Comments	FJ385I9C<H23HAAI2C
ProductName	24233HDH389D=D97H<I44?<
ProductVersion	4.7.9.11
FileDescription	24233HDH389D=D97H<I44?<
OriginalFilename	New Order 632487 PDF.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:27:38.506474972 CET	49724	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:27:41.621108055 CET	49724	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:27:47.621624947 CET	49724	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:27:56.288351059 CET	49728	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:27:59.294507027 CET	49728	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:05.310722113 CET	49728	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:13.285882950 CET	49729	7767	192.168.2.3	193.218.118.85

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:28:16.295875072 CET	49729	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:22.296358109 CET	49729	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:29.953555107 CET	49741	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:32.953835011 CET	49741	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:38.954144955 CET	49741	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:46.618545055 CET	49742	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:49.751879930 CET	49742	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:28:55.752271891 CET	49742	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:29:03.317387104 CET	49746	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:29:06.331403971 CET	49746	7767	192.168.2.3	193.218.118.85
Feb 24, 2021 08:29:12.331844091 CET	49746	7767	192.168.2.3	193.218.118.85

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:26:51.813945055 CET	56777	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:26:51.819036007 CET	58643	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:26:51.862639904 CET	53	56777	8.8.8.8	192.168.2.3
Feb 24, 2021 08:26:51.867713928 CET	53	58643	8.8.8.8	192.168.2.3
Feb 24, 2021 08:26:51.984157085 CET	60985	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:26:52.033083916 CET	53	60985	8.8.8.8	192.168.2.3
Feb 24, 2021 08:26:56.214761019 CET	50200	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:26:56.277456999 CET	53	50200	8.8.8.8	192.168.2.3
Feb 24, 2021 08:26:59.755116940 CET	51281	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:26:59.806962013 CET	53	51281	8.8.8.8	192.168.2.3
Feb 24, 2021 08:26:59.839361906 CET	49199	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:26:59.890907049 CET	53	49199	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:01.059406042 CET	50620	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:01.108555079 CET	53	50620	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:02.359008074 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:02.410617113 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:03.711429119 CET	60152	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:03.763259888 CET	53	60152	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:05.294286966 CET	57544	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:05.343498945 CET	53	57544	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:06.518959999 CET	55984	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:06.570784092 CET	53	55984	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:07.732810020 CET	64185	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:07.792707920 CET	53	64185	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:08.907334089 CET	65110	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:08.959305048 CET	53	65110	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:10.486464977 CET	58361	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:10.535645008 CET	53	58361	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:11.738147974 CET	63492	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:11.787111044 CET	53	63492	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:12.904726028 CET	60831	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:12.953589916 CET	53	60831	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:14.945636988 CET	60100	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:14.994864941 CET	53	60100	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:16.199708939 CET	60100	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:16.248699903 CET	53	60100	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:18.545169115 CET	53195	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:18.594221115 CET	53	53195	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:19.186659098 CET	50141	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:19.245006084 CET	53	50141	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:19.503521919 CET	53023	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:19.552885056 CET	53	53023	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:20.226172924 CET	49563	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:20.290333986 CET	53	49563	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:20.747888088 CET	51352	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:20.799860001 CET	53	51352	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:21.737982035 CET	59349	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:21.786956072 CET	53	59349	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:22.680237055 CET	57084	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:27:22.730372906 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:23.680464983 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:23.729445934 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:24.589320898 CET	57568	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:24.638376951 CET	53	57568	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:27.690359116 CET	50540	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:27.739727974 CET	53	50540	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:38.429212093 CET	54366	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:38.489042997 CET	53	54366	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:38.703165054 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:38.752595901 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:47.147347927 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:47.199500084 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 08:27:56.225450039 CET	55435	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:27:56.286724091 CET	53	55435	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:13.220204115 CET	50713	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:13.272465944 CET	53	50713	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:17.693212032 CET	56132	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:17.745332956 CET	53	56132	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:28.852796078 CET	58987	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:28.914611101 CET	53	58987	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:29.890443087 CET	56579	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:29.952094078 CET	53	56579	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:46.555999041 CET	60633	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:46.616513014 CET	53	60633	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:49.896667004 CET	61292	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:49.954571009 CET	53	61292	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:55.829619884 CET	63619	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:55.878711939 CET	53	63619	8.8.8.8	192.168.2.3
Feb 24, 2021 08:28:57.710882902 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:28:57.773530960 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 08:29:03.257323980 CET	61946	53	192.168.2.3	8.8.8.8
Feb 24, 2021 08:29:03.316689014 CET	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 08:27:38.429212093 CET	192.168.2.3	8.8.8.8	0xa07b	Standard query (0)	forcesbots .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:27:56.225450039 CET	192.168.2.3	8.8.8.8	0xbcc1	Standard query (0)	forcesbots .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:28:13.220204115 CET	192.168.2.3	8.8.8.8	0xd233	Standard query (0)	forcesbots .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:28:29.890443087 CET	192.168.2.3	8.8.8.8	0xcfb3	Standard query (0)	forcesbots .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:28:46.555999041 CET	192.168.2.3	8.8.8.8	0x3bf9	Standard query (0)	forcesbots .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:29:03.257323980 CET	192.168.2.3	8.8.8.8	0x2158	Standard query (0)	forcesbots .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

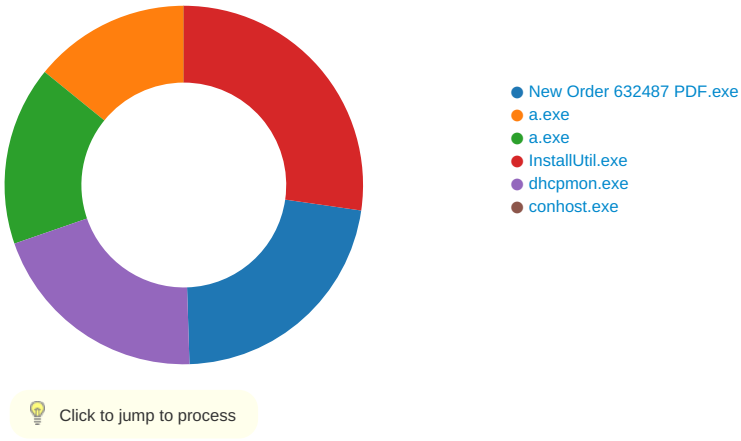
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 08:27:38.489042997 CET	8.8.8.8	192.168.2.3	0xa07b	No error (0)	forcesbots .ddns.net		193.218.118.85	A (IP address)	IN (0x0001)
Feb 24, 2021 08:27:56.286724091 CET	8.8.8.8	192.168.2.3	0xbcc1	No error (0)	forcesbots .ddns.net		193.218.118.85	A (IP address)	IN (0x0001)
Feb 24, 2021 08:28:13.272465944 CET	8.8.8.8	192.168.2.3	0xd233	No error (0)	forcesbots .ddns.net		193.218.118.85	A (IP address)	IN (0x0001)
Feb 24, 2021 08:28:29.952094078 CET	8.8.8.8	192.168.2.3	0xcfb3	No error (0)	forcesbots .ddns.net		193.218.118.85	A (IP address)	IN (0x0001)
Feb 24, 2021 08:28:46.616513014 CET	8.8.8.8	192.168.2.3	0x3bf9	No error (0)	forcesbots .ddns.net		193.218.118.85	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 08:29:03.316689014 CET	8.8.8.8	192.168.2.3	0x2158	No error (0)	forcesbots .ddns.net		193.218.118.85	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: New Order 632487 PDF.exe PID: 6284 Parent PID: 5600

General

Start time:	08:26:58
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\New Order 632487 PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order 632487 PDF.exe'
Imagebase:	0x1a0000
File size:	830976 bytes
MD5 hash:	6BB37FBE7FF7B15C6B20A788BA9D46FF
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: 00000000.00000002.285863508.00000000040C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.285863508.00000000040C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.285863508.00000000040C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.286576608.00000000041C6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.286576608.00000000041C6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.286576608.00000000041C6000.00000004.00000001.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	6DEBCF06	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	6DEBCF06	unknown
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	721AC82	CopyFileExW
C:\Users\user\AppData\Roaming\a.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	721AC82	CopyFileExW
C:\Users\user\AppData\Roaming\a.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	721AC82	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order 632487 PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	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 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 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	721AC82	CopyFileExW
C:\Users\user\AppData\Roaming\a.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 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 f2 bf 48 5e 00 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 50 00 00 a2 0c 00 00 0a 00 00 00 00 00 00 be c1 0c 00 00 20 00 00 00 e0 0c 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 00 20 0d 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.....H^.......... "...P.................. ....@.. ....`.................	success or wait	4	721AC82	CopyFileExW
C:\Users\user\AppData\Roaming\a.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	721AC82	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order 632487 PDF.exe.log	unknown	1128	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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 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 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1CC907	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: a.exe PID: 7084 Parent PID: 3388

General

Start time:	08:27:17

Start date:	24/02/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x380000
File size:	830976 bytes
MD5 hash:	6BB37FBE7FF7B15C6B20A788BA9D46FF
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: 00000006.00000002.500185390.0000000003705000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.500185390.0000000003705000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.500185390.0000000003705000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.500785518.00000000038BA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.500785518.00000000038BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.500785518.00000000038BA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.500410926.00000000037BD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.500410926.00000000037BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.500410926.00000000037BD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, Metadefender, Browse • Detection: 83%, 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	6DEBCF06	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	6DEBCF06	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: a.exe PID: 6132 Parent PID: 6284

General

Start time:	08:27:25
Start date:	24/02/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x820000
File size:	830976 bytes
MD5 hash:	6BB37FBE7FF7B15C6B20A788BA9D46FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6DEBCF06	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	6DEBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	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\a.exe.log	unknown	1128	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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 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 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1CC907	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: InstallUtil.exe PID: 6160 Parent PID: 7084

General

Start time:	08:27:28
Start date:	24/02/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x6a0000
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: 00000009.00000002.499062665.0000000003969000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.499062665.0000000003969000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.487651546.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.487651546.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.487651546.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.502699733.0000000005290000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.502699733.0000000005290000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.502699733.0000000005290000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.502105308.0000000005060000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.502105308.0000000005060000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.493457156.0000000002921000.00000004.00000001.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	6DEBCF06	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	6DEBCF06	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	6CD0BEFF	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	6CD01E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD0BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	6CD0DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CD0BEFF	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	6CD0BEFF	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	6b c1 d3 18 e1 d8 d8 48	k......H	success or wait	1	6CD01B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	41064	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6CD0DD66	CopyFileW

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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DE7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DE7D72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	4096	success or wait	1	6DE7D72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	512	success or wait	1	6DE7D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6CD0646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 5440 Parent PID: 3388

General

Start time:	08:27:45
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x790000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	132	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 75 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Installation utility Version 4. 7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CD01B4F	WriteFile
\Device\ConDrv	unknown	256	55 73 61 67 65 3a 20 49 6e 73 74 61 6c 6c 55 74 69 6c 20 5b 2f 75 20 7c 20 2f 75 6e 69 6e 73 74 61 6c 6c 5d 20 5b 6f 70 74 69 6f 6e 20 5b 2e 2e 2e 5d 5d 20 61 73 73 65 6d 62 6c 79 20 5b 5b 6f 70 74 69 6f 6e 20 5b 2e 2e 2e 5d 5d 20 61 73 73 65 6d 62 6c 79 5d 20 5b 2e 2e 2e 5d 5d 0d 0a 0d 0a 49 6e 73 74 61 6c 6c 55 74 69 6c 20 65 78 65 63 75 74 65 73 20 74 68 65 20 69 6e 73 74 61 6c 6c 65 72 73 20 69 6e 20 65 61 63 68 20 67 69 76 65 6e 20 61 73 73 65 6d 62 6c 79 2e 0d 0a 49 66 20 74 68 65 20 2f 75 20 6f 72 20 2f 75 6e 69 6e 73 74 61 6c 6c 20 73 77 69 74 63 68 20 69 73 20 73 70 65 63 69 66 69 65 64 2c 20 69 74 20 75 6e 69 6e 73 74 61 6c 6c 73 0d 0a 74 68 65 20 61 73 73 65 6d 62 6c 69 65 73 2c 20 6f 74 68 65 72 77 69 73 65 20 69 74 20 69 6e 73 74 61 6c 6c 73	Usage: InstallUtil [/u | /uninstall] [option [...]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs	success or wait	7	6CD01B4F	WriteFile
\Device\ConDrv	unknown	93	69 74 68 20 74 68 65 20 70 61 74 68 73 0d 0a 6f 66 20 74 68 65 20 61 73 73 65 6d 62 6c 69 65 73 20 6f 6e 20 74 68 65 20 63 6f 6d 6d 61 6e 64 20 6c 69 6e 65 20 61 6c 6f 6e 67 20 77 69 74 68 20 74 68 65 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 6f 70 74 69 6f 6e 2e 0d 0a 0d 0a 0d 0a	ith the paths..of the assemblies on the command line along with the /? or /help option.....	success or wait	1	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	950	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 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 49 6e 73 74 61 6c 6c 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 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImage	success or wait	1	6E1CC907	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: conhost.exe PID: 6340 Parent PID: 5440

General

Start time:	08:27:46
Start date:	24/02/2021
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

Disassembly

Code Analysis