ID: 355753
Sample Name:
256ec8f8f67b59c5e085b0bb63afcd13.exe
Cookbook: default.jbs
Time: 19:09:11
Date: 21/02/2021
Version: 31.0.0 Emerald

Table of Contents

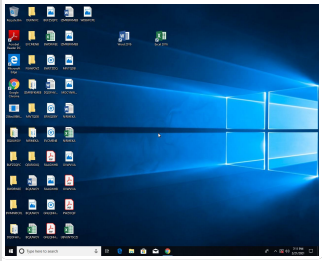
Analysis Report 256ec8f8f67b59c5e085b0bb63afcd13.exe

Overview

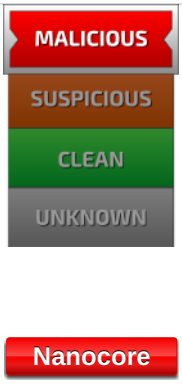
General Information

Sample Name:	256ec8f8f67b59c5e085b0bb63afcd13.exe
Analysis ID:	355753
MD5:	0bbcc2e64e3edf0..
SHA1:	c006b8d2ec4b92..
SHA256:	52d01903f7c366e.
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



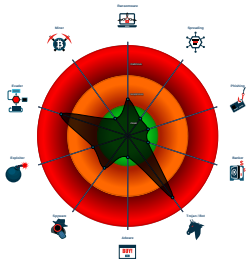
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Uses schtasks.exe or at.exe to add …

Classification



Startup

- **System is w10x64**
- 256ec8f8f67b59c5e085b0bb63afcd13.exe (PID: 6720 cmdline: 'C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe' MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
  - 256ec8f8f67b59c5e085b0bb63afcd13.exe (PID: 6416 cmdline: {path} MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
    - schtasks.exe (PID: 6540 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp98F0.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6632 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpA082.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 256ec8f8f67b59c5e085b0bb63afcd13.exe (PID: 6888 cmdline: C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe 0 MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
  - 256ec8f8f67b59c5e085b0bb63afcd13.exe (PID: 6260 cmdline: {path} MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
- dhcpmon.exe (PID: 2460 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
  - dhcpmon.exe (PID: 6500 cmdline: {path} MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
- dhcpmon.exe (PID: 7160 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
  - dhcpmon.exe (PID: 5748 cmdline: {path} MD5: 0BBCC2E64E3EDF053ED4AF2C0BAFB0EB)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "94----",
  "Group": "V-HASH",
  "Domain1": "cloudhost.myfirewall.org",
  "Domain2": "cloudhost.myfirewall.org",
  "Port": 5654,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "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": "cloudhost.myfirewall.org",
  "BackupDNSServer": "cloudhost.myfirewall.orgbxpU=",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.721135661.000000000347 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.721135661.000000000347 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x23877:$a: NanoCore • 0x238d0:$a: NanoCore • 0x2390d:$a: NanoCore • 0x23986:$a: NanoCore • 0x238d9:$b: ClientPlugin • 0x23916:$b: ClientPlugin • 0x24214:$b: ClientPlugin • 0x24221:$b: ClientPlugin • 0x1b5fe:$e: KeepAlive • 0x23d61:$g: LogClientMessage • 0x23ce1:$i: get_Connected • 0x158a9:$j: #=q • 0x158d9:$j: #=q • 0x15915:$j: #=q • 0x1593d:$j: #=q • 0x1596d:$j: #=q • 0x1599d:$j: #=q • 0x159cd:$j: #=q • 0x159fd:$j: #=q • 0x15a19:$j: #=q • 0x15a49:$j: #=q
00000008.00000002.717514074.0000000003B5 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x23761d:$x1: NanoCore.ClientPluginHost • 0x26a03d:$x1: NanoCore.ClientPluginHost • 0x23765a:$x2: IClientNetworkHost • 0x26a07a:$x2: IClientNetworkHost • 0x23b18d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x26dbad:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.717514074.0000000003B5 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.717514074.0000000003B5 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x237385:$a: NanoCore • 0x237395:$a: NanoCore • 0x2375c9:$a: NanoCore • 0x2375dd:$a: NanoCore • 0x23761d:$a: NanoCore • 0x269da5:$a: NanoCore • 0x269db5:$a: NanoCore • 0x269fe9:$a: NanoCore • 0x269ffd:$a: NanoCore • 0x26a03d:$a: NanoCore • 0x2373e4:$b: ClientPlugin • 0x2375e6:$b: ClientPlugin • 0x237626:$b: ClientPlugin • 0x269e04:$b: ClientPlugin • 0x26a006:$b: ClientPlugin • 0x26a046:$b: ClientPlugin • 0x1835a1:$c: ProjectData • 0x23750b:$c: ProjectData • 0x269f2b:$c: ProjectData • 0x237f12:$d: DESCrypto • 0x26a932:$d: DESCrypto
Click to see the 62 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
14.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
14.2.dhcpmon.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
14.2.dhcpmon.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
2.2.256ec8f8f67b59c5e085b0bb63afcd13.exe .405eab4.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 122 entries				

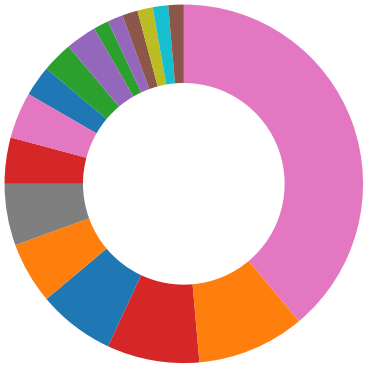
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

- Found malware configuration
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files
- Uses new MSVCR Dlls
- 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

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

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:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

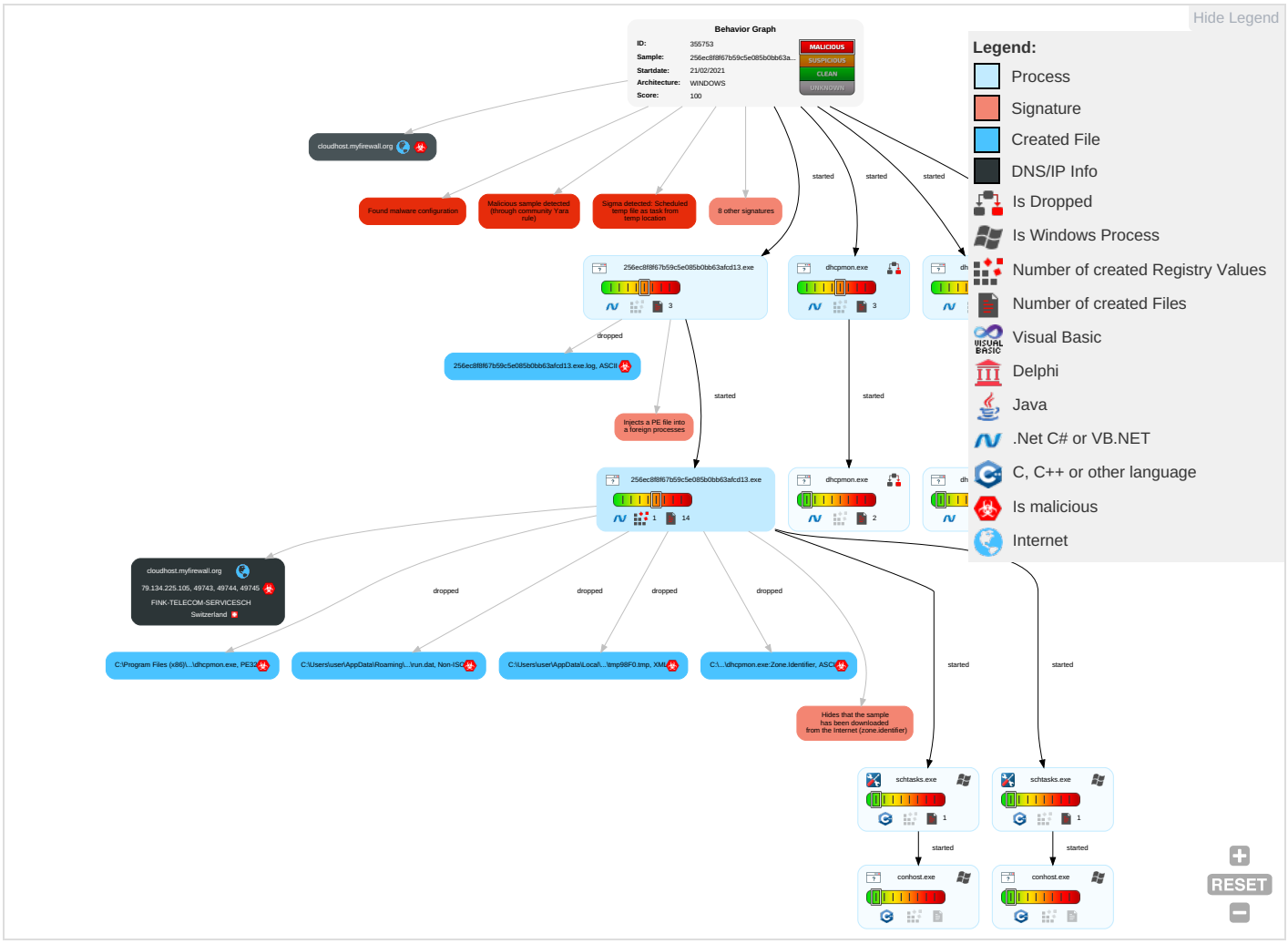
Detected Nanocore Rat

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	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 1 1	Security Software Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

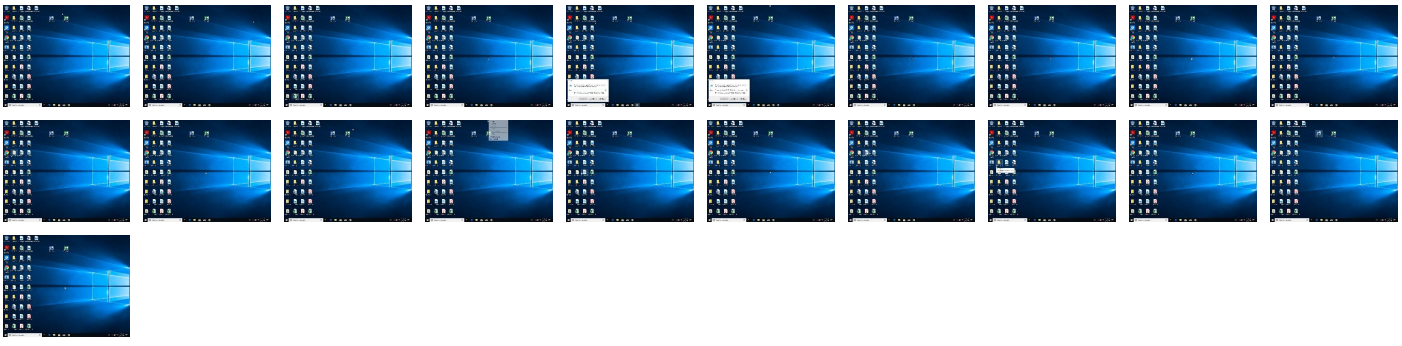
Behavior Graph



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
256ec8f8f67b59c5e085b0bb63afcd13.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.256ec8f8f67b59c5e085b0bb63afcd13.exe.5c20000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
12.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.256ec8f8f67b59c5e085b0bb63afcd13.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.256ec8f8f67b59c5e085b0bb63afcd13.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
cloudhost.myfirewall.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
cloudhost.myfirewall.org	1%	Virustotal		Browse
cloudhost.myfirewall.org	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.comFalMY~	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr~y8	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com;	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.comF	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypooo	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comypo	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comV	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comlay	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sandoll.co.krC	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.carterandcone.comgy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.fonts.comi	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcy5	0%	Avira URL Cloud	safe	
http://www.fonts.comWh2	0%	Avira URL Cloud	safe	
http://www.tiro.comalMY~	0%	Avira URL Cloud	safe	
http://www.fonts.comX	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFpz3	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.comalsekz	0%	Avira URL Cloud	safe	
http://www.carterandcone.comint	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn7	0%	Avira URL Cloud	safe	
http://www.fontbureau.commzN	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.carterandcone.comgne	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cloudhost.myfirewall.org	79.134.225.105	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
cloudhost.myfirewall.org	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comFalMY~	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638389150.0000000005569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers?	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr~y8	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638866258.0000000005686000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com;	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.637926766.000000000569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.tiro.comF	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638355631.000000000569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comypooo	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.640116720.00000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639713902.00000000056BE000.00000004.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639797895.0000000056BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersQ	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.642184941.00000000056B5000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comypo	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639797895.00000000056BE000.00000004.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639991224.0000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/mzN	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.643315337.0000000005684000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

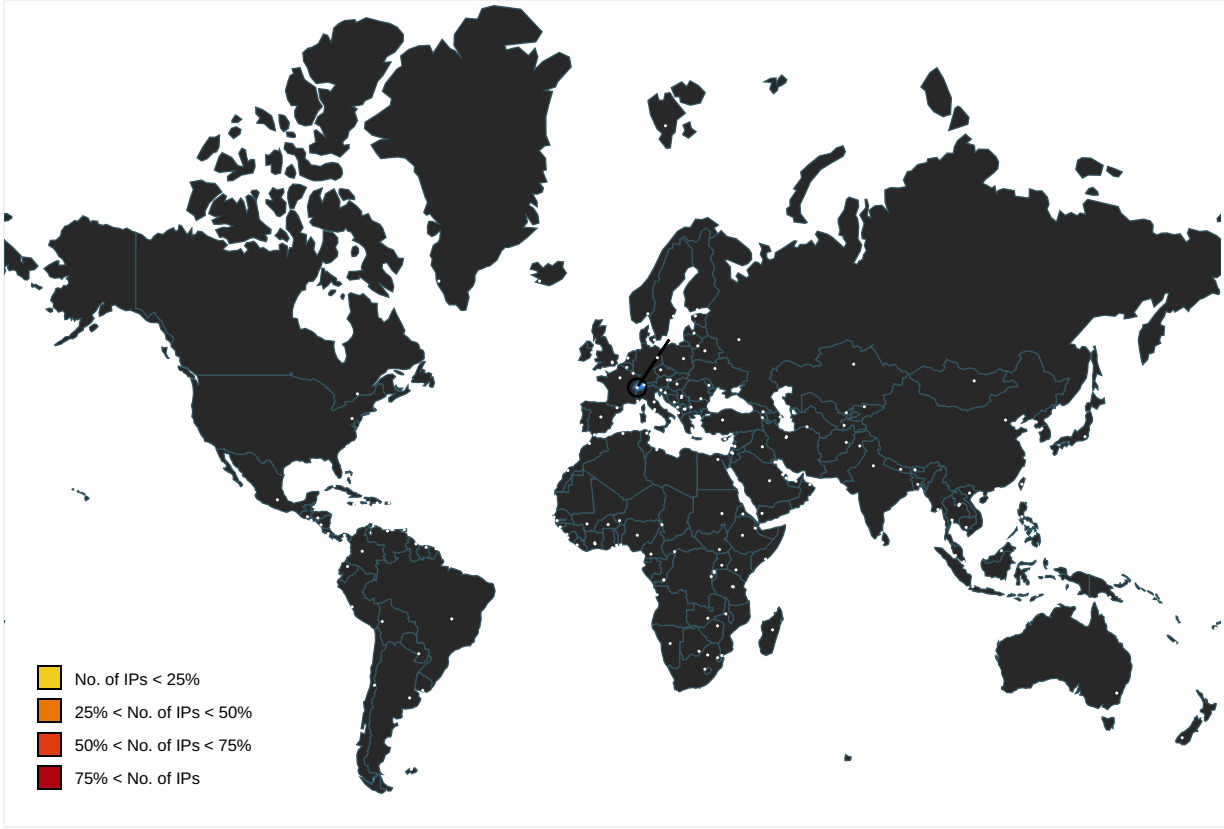
Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.0000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersb	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.643199147.00000000056B5000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.0000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comV	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639713902.00000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.0000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.0000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comlay	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639713902.00000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.0000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krC	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638866258.0000000005686000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersr	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.642893460.00000000056B5000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.644178396.000000000568D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comc	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638167842.000000000569B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comgy	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639918482.00000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639860700.00000000056BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comi	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638167842.000000000569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.htmln	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.642401940.00000000056B5000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comcy5	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639918482.00000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comWh2	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638167842.000000000569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comalMY~	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638412498.000000000569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fonts.comX	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.638167842.000000000569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comFpz3	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.643315337.0000000005684000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639394139.0000000005684000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comalsekz	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.643315337.0000000005684000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comint	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639713902.00000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers&	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.642010809.00000000056B5000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.677120512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639259634.0000000005684000.00000004.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639244161.00000000056BD000.00000004.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.6771 20512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn7	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639244161.00000000056BD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.commzN	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.676929479.0000000005680000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.676929479.0000000005680000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.6771 20512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.coma-d	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.637926766.000000000569B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/k	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.641965748.00000000056B5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000002.6771 20512.0000000005960000.00000002.00000001.sdmp, 256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000007.00000002.715867498.00000000059B0000.00000002.00000001.sdmp, dhcpmon.exe, 00000008.00000002.720166161.0000000004DB0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.732352387.0000000005A00000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers=	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.642184941.00000000056B5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comals	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.643315337.0000000005684000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comgne	256ec8f8f67b59c5e085b0bb63afcd13.exe, 00000000.00000003.639900319.00000000056BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.105	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355753
Start date:	21.02.2021
Start time:	19:09:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	256ec8f8f67b59c5e085b0bb63afcd13.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:	24
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@18/8@20/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 1.3% (good quality ratio 1.3%) • Quality average: 88.6% • Quality standard deviation: 6.7%
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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 168.61.161.212, 52.147.198.201, 40.126.31.137, 40.126.31.6, 20.190.159.138, 20.190.159.134, 40.126.31.8, 20.190.159.136, 40.126.31.1, 40.126.31.143, 93.184.220.29, 51.104.144.132, 13.107.4.50, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, Edge-Prod-FRA.env.au.au-msedge.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, afdap.au.au-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, au.au-msedge.net, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:09:59	API Interceptor	852x Sleep call for process: 256ec8f8f67b59c5e085b0bb63afcd13.exe modified
19:10:12	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
19:10:14	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe" s>$(Arg0)
19:10:14	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
19:10:15	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.105	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	
	73a4f40d0affe5eea89174f8917bba73.exe	Get hash	malicious	Browse	
	9a08c8a2b49d6348f2ef35f85a1c6351.exe	Get hash	malicious	Browse	
	7eec14e7cec4dc93fbf53e08998b2340.exe	Get hash	malicious	Browse	
	f2a22415c1b108ce91fd76e3320431d0.exe	Get hash	malicious	Browse	
	1d8eff2bc76e46dc186fa501e24f5cb1.exe	Get hash	malicious	Browse	
	1464bbe24dac1f403f15b3c3860f37ca.exe	Get hash	malicious	Browse	
	1d78424ce6944359d546dbcbc030f19e.exe	Get hash	malicious	Browse	
	84ab43f7eda35ae038b199d3a3586b77.exe	Get hash	malicious	Browse	
	Require_Quote_20200128 SSG.pdf ind.exe	Get hash	malicious	Browse	
	DHL FILE 987634732.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	NKF20205 LIST.exe	Get hash	malicious	Browse	
	URGENT PO.exe	Get hash	malicious	Browse	
	scan002947779488.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cloudhost.myfirewall.org	9a08c8a2b49d6348f2ef35f85a1c6351.exe	Get hash	malicious	Browse	• 79.134.225.105
	zSDBuG8gDl.exe	Get hash	malicious	Browse	• 185.229.243.67
	65d1beae1fc7eb126cd4a9b277afb942.exe	Get hash	malicious	Browse	• 79.134.225.96
	f2a22415c1b108ce91fd76e3320431d0.exe	Get hash	malicious	Browse	• 79.134.225.105
	1d8eff2bc76e46dc186fa501e24f5cb1.exe	Get hash	malicious	Browse	• 79.134.225.105
	5134b758f8eb77424254ce67f4697ffe.exe	Get hash	malicious	Browse	• 79.134.225.96
	1d8eff2bc76e46dc186fa501e24f5cb1.exe	Get hash	malicious	Browse	• 79.134.225.96
	460f7e6048ed3ca91f1573a7410fedd6.exe	Get hash	malicious	Browse	• 79.134.225.96
	1d78424ce6944359d546dbcbc030f19e.exe	Get hash	malicious	Browse	• 79.134.225.105

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	Solicitud de oferta 6100003768.exe	Get hash	malicious	Browse	• 79.134.225.96
	Nrfgylra.exe	Get hash	malicious	Browse	• 79.134.225.96
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	Form pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	Quotation 3342688.exe	Get hash	malicious	Browse	• 79.134.225.120
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 79.134.225.76
	Orden.exe	Get hash	malicious	Browse	• 79.134.225.6
	Ordine.exe	Get hash	malicious	Browse	• 79.134.225.11
	73a4f40d0affe5eea89174f8917bba73.exe	Get hash	malicious	Browse	• 79.134.225.105
	ToolNcatalogpri00088756564162021.exe	Get hash	malicious	Browse	• 79.134.225.45
	INV WJD000030036000137675999, xlsx.exe	Get hash	malicious	Browse	• 79.134.225.69
	Kreuzmayr_PO_22656_65564345565643ETD,pdf.exe	Get hash	malicious	Browse	• 79.134.225.73
	jYHhaKx7OH.exe	Get hash	malicious	Browse	• 79.134.225.96
	request.doc	Get hash	malicious	Browse	• 79.134.225.69

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	412672
Entropy (8bit):	7.944378053087377
Encrypted:	false
SSDEEP:	6144:x/7jHNyWI+b1m3N2teCoTpkB/Bm8V/7bLf8q2/MQo1m1dupfmndJLvG:fEaE3N20CBTHU/Noydupf2
MD5:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
SHA1:	C006B8D2EC4B92F441815B20F1BDADF98EAB1B4D
SHA-256:	52D01903F7C366E01359A00EA771CA1F71D4E1BB54731290BC62C3A218F5AF80
SHA-512:	0BED9AC8299A16BA8F9DEFA6160A97654B08C86BF038367FC5508A90240C5801320955DCA4D452FD7E41F16CC1A71A20AC0A946D80101DC65E9495C15F98EF3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..._h2`.....0..@.....j^... ...`....@.. ....@.....^..O...`.. ..... ..... ..H.....text...p>... ...@..... ..`.rsrc... ....`.....B.....@..@.rel oc.....J.....@..B.....L^.....H.....LQ..$>.....\...p.....0.....r...p.+..*..0.....r...p.+..*".(.....*^..}.....(.....(.....*.0.....s....%.{....o.. ..o.....+..*..*.0..+.....,.{.....+.....{....o.....(....*..0.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....{....o.....{....o.....(.....{....o.....{....o.....{....o.....{....o.....{.....s ...o!.....{....r...po".....{.... .....#s#...o$.....{.....o%.

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

Process:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\256ec8f8f67b59c5e085b0bb63afcd13.exe.log

Process:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp98F0.tmp	
Process:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.162258309875531
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0YbGPxtn:cbk4oL600QydbQxIYODOLedq3uj
MD5:	B78304EA0D7AFCCEFC8CFF617158D17C
SHA1:	76DD98BBFE885893DC19059C139EDCB829DFA21E
SHA-256:	B80490FC583697FD68F2B7D0986C9F3BA3944BDB9AEA7F17C826E26BF1749C7F
SHA-512:	44682D75002B56551B4075616110FF4887DD298D7B9B96A312BDDAB6AB94A7E42AFADF690CED378FF403337185DD74C77D2B4DABE3BB60B9642C24079AC5106
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpA082.tmp	
Process:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:JPn:JPn
MD5:	5BF06D5C11AE13FC9970936540EB0703
SHA1:	54B778FC0BA984A04D47CB1E5C6E8252E9BE3FF9
SHA-256:	39974C521C78E35079501265DF5A694586DAB94A7EE52F6E923756C5AFE5F3F0
SHA-512:	C0CF94EB89C82DD4D0B9F798D1C30D02F93C8A02C526F5605356F649259F23ED47820D99F10B94A34929EC144835D9F389121AEF98E55EB5CB30CCBFF6B0FC3
Malicious:	**true**
Preview:	.>....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.5831339906659565
Encrypted:	false
SSDEEP:	3:oNt+WfWXQj0l/sPDWsC:oNwvAj0Gs7lC
MD5:	90C08D85024FAD583545EC9562AA4A7E
SHA1:	FB6483F47BEC7ED49479D276986B4B789D9725AD
SHA-256:	28D29127F67EA98D32833FAC5491366FEC57805EAFF2B15A8AB9AF2555EADCA3
SHA-512:	EEC099998337F7294CFA0C273BFC1D31CDBA555935163CC483E00D7451A529ECF71131EAB74549B031EA9F6A15531F68D5CA1A4070D3EB7B97E5CC13D1701C7
Malicious:	false
Preview:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.944378053087377
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	256ec8f8f67b59c5e085b0bb63afcd13.exe
File size:	412672
MD5:	0bbcc2e64e3edf053ed4af2c0bafb0eb
SHA1:	c006b8d2ec4b92f441815b20f1bdadf98eab1b4d
SHA256:	52d01903f7c366e01359a00ea771ca1f71d4e1bb5473129 0bc62c3a218f5af80
SHA512:	0bed9ac8299a16ba8f9defa6160a97654b08c86bf038367 fc5508a90240c5801320955dca4d452fd7e41f16cc1a71a 20ac0a946d80101dc65e9495c15f98ef3c
SSDEEP:	6144:x/7jHNyWI+b1m3N2teCoTpkB/Bm8V/7bLf8q2/MQ o1m1dupfmndJLvG:fEaE3N20CBTHU/Noydupf2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..._h2`.....0..@.....j^... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x465e6a
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
Time Stamp:	0x6032685F [Sun Feb 21 14:04:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x65e18	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x66000	0x620	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	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	0x63e70	0x64000	False	0.948125	data	7.95731162888	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x66000	0x620	0x800	False	0.3427734375	data	3.56974614095	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x68000	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_VERSION	0x66090	0x390	data		
RT_MANIFEST	0x66430	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

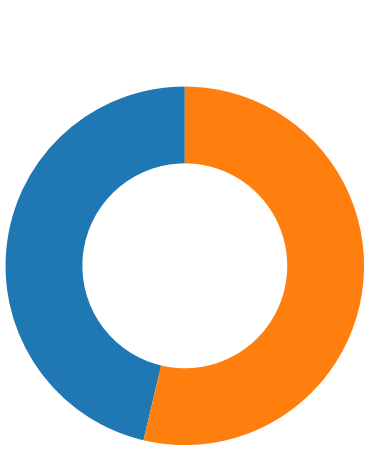
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	2013-2021 (C) Blackboard Learn
Assembly Version	16.60.0.4
InternalName	0FDM.exe
FileVersion	16.69.0.4
CompanyName	Blackboard Learn
LegalTrademarks	
Comments	Moodle
ProductName	Student Studio
ProductVersion	16.69.0.4
FileDescription	Student Studio
OriginalFilename	0FDM.exe

Network Behavior

Network Port Distribution

Total Packets: 108

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 19:10:14.481653929 CET	49743	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:14.565690994 CET	5654	49743	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:15.072868109 CET	49743	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:15.159531116 CET	5654	49743	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:15.664880037 CET	49743	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:15.747469902 CET	5654	49743	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:19.969670057 CET	49744	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:20.058454990 CET	5654	49744	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:20.618283033 CET	49744	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:20.703840017 CET	5654	49744	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:21.212810993 CET	49744	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:21.301839113 CET	5654	49744	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:25.510416985 CET	49745	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:25.595660925 CET	5654	49745	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:26.196866989 CET	49745	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:26.282290936 CET	5654	49745	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:26.884773016 CET	49745	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:26.970243931 CET	5654	49745	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:31.217709064 CET	49746	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:31.301038027 CET	5654	49746	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:31.816807032 CET	49746	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:31.899502993 CET	5654	49746	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:32.416230917 CET	49746	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:32.501424074 CET	5654	49746	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:36.666985035 CET	49751	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:36.751816034 CET	5654	49751	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:37.307209015 CET	49751	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:37.393260002 CET	5654	49751	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:37.916681051 CET	49751	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:38.001872063 CET	5654	49751	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:42.088305950 CET	49752	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:42.175749063 CET	5654	49752	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:42.682614088 CET	49752	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:42.768296957 CET	5654	49752	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:43.276427984 CET	49752	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:43.364061117 CET	5654	49752	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:48.494093895 CET	49754	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:48.576904058 CET	5654	49754	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:49.089562893 CET	49754	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:49.172209024 CET	5654	49754	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:49.683207989 CET	49754	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:49.765983105 CET	5654	49754	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:53.863328934 CET	49755	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:53.950566053 CET	5654	49755	79.134.225.105	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 19:10:54.464886904 CET	49755	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:54.550196886 CET	5654	49755	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:55.058656931 CET	49755	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:55.144181013 CET	5654	49755	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:59.228866100 CET	49764	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:59.318568945 CET	5654	49764	79.134.225.105	192.168.2.4
Feb 21, 2021 19:10:59.825444937 CET	49764	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:10:59.908130884 CET	5654	49764	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:00.418479919 CET	49764	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:00.504683018 CET	5654	49764	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:04.667921066 CET	49768	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:04.753856897 CET	5654	49768	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:05.262670040 CET	49768	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:05.377309084 CET	5654	49768	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:05.887820959 CET	49768	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:05.970722914 CET	5654	49768	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:10.697511911 CET	49772	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:10.784476042 CET	5654	49772	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:11.294397116 CET	49772	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:11.388797998 CET	5654	49772	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:11.904058933 CET	49772	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:11.988487959 CET	5654	49772	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:16.086658955 CET	49775	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:16.169102907 CET	5654	49775	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:16.669847012 CET	49775	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:16.762417078 CET	5654	49775	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:17.263628960 CET	49775	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:17.346447945 CET	5654	49775	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:21.496545076 CET	49776	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:21.582596064 CET	5654	49776	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:22.092253923 CET	49776	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:22.179691076 CET	5654	49776	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:22.685975075 CET	49776	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:22.773654938 CET	5654	49776	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:26.892983913 CET	49777	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:26.977591991 CET	5654	49777	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:27.483406067 CET	49777	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:27.567987919 CET	5654	49777	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:28.077723980 CET	49777	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:28.160851002 CET	5654	49777	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:32.253349066 CET	49778	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:32.341033936 CET	5654	49778	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:32.843106031 CET	49778	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:32.946002960 CET	5654	49778	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:33.452650070 CET	49778	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:33.540216923 CET	5654	49778	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:37.963520050 CET	49779	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:38.048171043 CET	5654	49779	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:38.577904940 CET	49779	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:38.662389040 CET	5654	49779	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:39.171739101 CET	49779	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:39.258052111 CET	5654	49779	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:43.969376087 CET	49780	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:44.054805994 CET	5654	49780	79.134.225.105	192.168.2.4
Feb 21, 2021 19:11:44.562824965 CET	49780	5654	192.168.2.4	79.134.225.105
Feb 21, 2021 19:11:44.648353100 CET	5654	49780	79.134.225.105	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 19:09:48.930857897 CET	54531	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:48.982146978 CET	53	54531	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:49.823251963 CET	49714	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:49.871979952 CET	53	49714	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 19:09:51.212296963 CET	58028	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:51.260798931 CET	53	58028	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:52.114397049 CET	53097	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:52.168731928 CET	53	53097	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:53.199487925 CET	49257	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:53.249475002 CET	53	49257	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:54.438493967 CET	62389	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:54.491493940 CET	53	62389	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:55.249241114 CET	49910	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:55.298619032 CET	53	49910	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:56.177673101 CET	55854	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:56.229222059 CET	53	55854	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:57.144870043 CET	64549	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:57.196521044 CET	53	64549	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:58.704134941 CET	63153	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:58.752796888 CET	53	63153	8.8.8.8	192.168.2.4
Feb 21, 2021 19:09:59.582113028 CET	52991	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:09:59.631140947 CET	53	52991	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:00.345346928 CET	53700	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:00.396811008 CET	53	53700	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:01.173523903 CET	51726	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:01.225342989 CET	53	51726	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:02.044966936 CET	56794	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:02.093724966 CET	53	56794	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:03.014596939 CET	56534	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:03.064789057 CET	53	56534	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:03.832214117 CET	56627	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:03.884660959 CET	53	56627	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:04.691565037 CET	56621	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:04.742393970 CET	53	56621	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:05.521996021 CET	63116	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:05.571896076 CET	53	63116	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:14.237704992 CET	64078	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:14.307945013 CET	53	64078	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:19.900085926 CET	64801	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:19.956199884 CET	53	64801	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:25.420279980 CET	61721	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:25.490183115 CET	53	61721	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:31.005204916 CET	51255	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:31.065110922 CET	53	51255	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:32.919872046 CET	61522	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:32.982388973 CET	53	61522	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:33.138350964 CET	52337	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:33.191318989 CET	53	52337	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:33.450341940 CET	55046	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:33.501333952 CET	53	55046	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:36.605760098 CET	49612	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:36.665493011 CET	53	49612	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:42.038508892 CET	49285	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:42.087125063 CET	53	49285	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:43.471916914 CET	50601	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:43.520714045 CET	53	50601	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:48.389977932 CET	60875	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:48.440829992 CET	53	60875	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:53.801810980 CET	56448	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:53.860038996 CET	53	56448	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:54.833420992 CET	59172	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:54.928378105 CET	53	59172	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:55.452928066 CET	62420	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:55.510045052 CET	53	62420	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:56.095340014 CET	60579	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:56.144824028 CET	53	60579	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:56.231909037 CET	50183	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:56.306546926 CET	53	50183	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 19:10:56.870721102 CET	61531	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:56.919975996 CET	53	61531	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:57.407344103 CET	49228	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:57.497565031 CET	53	49228	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:58.045015097 CET	59794	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:58.133251905 CET	53	59794	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:58.729538918 CET	55916	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:58.795614958 CET	53	55916	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:59.175395966 CET	52752	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:59.227727890 CET	53	52752	8.8.8.8	192.168.2.4
Feb 21, 2021 19:10:59.520904064 CET	60542	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:10:59.570298910 CET	53	60542	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:00.651365995 CET	60689	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:00.708756924 CET	53	60689	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:01.183861017 CET	64206	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:01.243877888 CET	53	64206	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:04.595330954 CET	50904	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:04.662915945 CET	53	50904	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:09.863444090 CET	57525	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:09.914339066 CET	53	57525	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:09.970029116 CET	53814	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:10.047624111 CET	53	53814	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:10.646823883 CET	53418	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:10.696320057 CET	53	53418	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:11.946039915 CET	62833	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:12.011301041 CET	53	62833	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:16.027312040 CET	59260	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:16.085422993 CET	53	59260	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:21.439564943 CET	49944	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:21.494040966 CET	53	49944	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:26.815378904 CET	63300	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:26.889494896 CET	53	63300	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:32.201236010 CET	61449	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:32.251133919 CET	53	61449	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:37.896838903 CET	51275	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:37.962276936 CET	53	51275	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:43.917714119 CET	63492	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:43.968136072 CET	53	63492	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:45.245934963 CET	58945	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:45.295686960 CET	53	58945	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:49.000189066 CET	60779	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:49.059232950 CET	53	60779	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:49.281303883 CET	64014	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:49.329972982 CET	53	64014	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:54.650861025 CET	57091	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:11:54.702620029 CET	53	57091	8.8.8.8	192.168.2.4
Feb 21, 2021 19:11:59.986953974 CET	55904	53	192.168.2.4	8.8.8.8
Feb 21, 2021 19:12:00.047180891 CET	53	55904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 21, 2021 19:10:14.237704992 CET	192.168.2.4	8.8.8.8	0x58b3	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:19.900085926 CET	192.168.2.4	8.8.8.8	0x2e69	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:25.420279980 CET	192.168.2.4	8.8.8.8	0xc51	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:31.005204916 CET	192.168.2.4	8.8.8.8	0x9380	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:36.605760098 CET	192.168.2.4	8.8.8.8	0x18db	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:42.038508892 CET	192.168.2.4	8.8.8.8	0xbe86	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:48.389977932 CET	192.168.2.4	8.8.8.8	0x5bdf	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 21, 2021 19:10:53.801810980 CET	192.168.2.4	8.8.8.8	0x5d7e	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:59.175395966 CET	192.168.2.4	8.8.8.8	0x964c	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:04.595330954 CET	192.168.2.4	8.8.8.8	0xce78	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:10.646823883 CET	192.168.2.4	8.8.8.8	0x80ee	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:16.027312040 CET	192.168.2.4	8.8.8.8	0x831c	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:21.439564943 CET	192.168.2.4	8.8.8.8	0xdff9	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:26.815378904 CET	192.168.2.4	8.8.8.8	0x9982	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:32.201236010 CET	192.168.2.4	8.8.8.8	0x54b7	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:37.896838903 CET	192.168.2.4	8.8.8.8	0x429e	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:43.917714119 CET	192.168.2.4	8.8.8.8	0xcd9d	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:49.281303883 CET	192.168.2.4	8.8.8.8	0x2942	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:54.650861025 CET	192.168.2.4	8.8.8.8	0x7fae	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:59.986953974 CET	192.168.2.4	8.8.8.8	0x3e30	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

DNS Answers

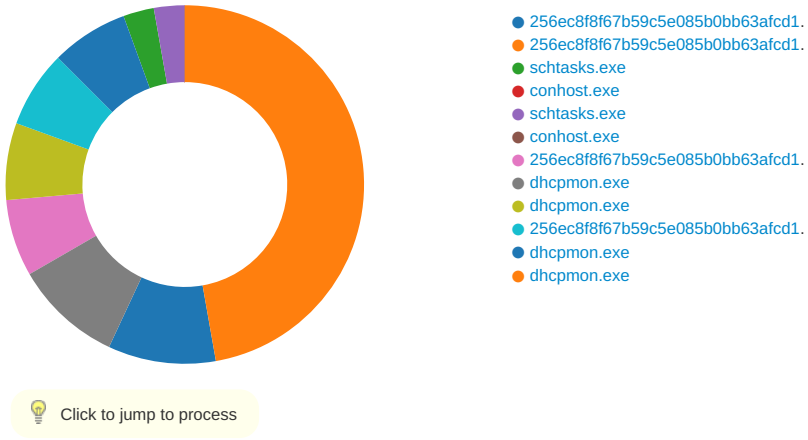
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 21, 2021 19:10:14.307945013 CET	8.8.8.8	192.168.2.4	0x58b3	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:19.956199884 CET	8.8.8.8	192.168.2.4	0x2e69	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:25.490183115 CET	8.8.8.8	192.168.2.4	0xc51	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:31.065110922 CET	8.8.8.8	192.168.2.4	0x9380	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:32.982388973 CET	8.8.8.8	192.168.2.4	0x73f3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 21, 2021 19:10:36.665493011 CET	8.8.8.8	192.168.2.4	0x18db	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:42.087125063 CET	8.8.8.8	192.168.2.4	0xbe86	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:48.440829992 CET	8.8.8.8	192.168.2.4	0x5bdf	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:53.860038996 CET	8.8.8.8	192.168.2.4	0x5d7e	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:10:59.227727890 CET	8.8.8.8	192.168.2.4	0x964c	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:04.662915945 CET	8.8.8.8	192.168.2.4	0xce78	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:10.696320057 CET	8.8.8.8	192.168.2.4	0x80ee	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:16.085422993 CET	8.8.8.8	192.168.2.4	0x831c	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:21.494040966 CET	8.8.8.8	192.168.2.4	0xdff9	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:26.889494896 CET	8.8.8.8	192.168.2.4	0x9982	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 21, 2021 19:11:32.251133919 CET	8.8.8.8	192.168.2.4	0x54b7	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:37.962276936 CET	8.8.8.8	192.168.2.4	0x429e	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:43.968136072 CET	8.8.8.8	192.168.2.4	0xcd9d	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:49.329972982 CET	8.8.8.8	192.168.2.4	0x2942	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:11:54.702620029 CET	8.8.8.8	192.168.2.4	0x7fae	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 21, 2021 19:12:00.047180891 CET	8.8.8.8	192.168.2.4	0x3e30	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 256ec8f8f67b59c5e085b0bb63afcd13.exe PID: 6720 Parent PID: 6088

General

Start time:	19:09:54
Start date:	21/02/2021
Path:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe'
Imagebase:	0xc40000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB

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: 00000000.00000002.676219646.00000000042A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.676219646.00000000042A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.676219646.00000000042A1000.00000004.00000001.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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\256ec8f8f67b59c5e085b0bb63afcd13.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\256ec8f8f67b59c5e085b0bb63afcd13.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: 256ec8f8f67b59c5e085b0bb63afcd13.exe PID: 6416 Parent PID: 6720

General

Start time:	19:10:08
Start date:	21/02/2021
Path:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8f0000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
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: 00000002.00000002.907132131.0000000005980000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.907132131.0000000005980000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.907264968.0000000005C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.907264968.0000000005C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.907264968.0000000005C20000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.903845537.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.903845537.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.903845537.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.905880969.0000000004057000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.905880969.0000000004057000.00000004.00000001.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	722760AC	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	722760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	52507A1	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	525089B	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	52507A1	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	5250B20	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5250B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp98F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5250D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	525089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA082.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5250D1C	GetTempFileNameW
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	52507A1	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	52507A1	CreateDirectoryW
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	722760AC	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	722760AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp98F0.tmp	success or wait	1	71857D95	unknown
C:\Users\user\AppData\Local\Temp\tmpA082.tmp	success or wait	1	71857D95	unknown
C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe:Zone.Identifier	success or wait	1	525114D	DeleteFileA

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	da 3e 8c ed 93 d6 d8 48	.>.....H	success or wait	1	5250A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5f 68 32 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 40 06 00 00 0a 00 00 00 00 00 00 6a 5e 06 00 00 20 00 00 00 60 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 06 00 00 02 00 00 00 00 00 00 02 00 40 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..._h2`.......... ....0..@..........j^... ...`....@.. ....@.................	success or wait	4	5250B20	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.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	5250B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp98F0.tmp	unknown	1322	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	5250A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	59	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 32 35 36 65 63 38 66 38 66 36 37 62 35 39 63 35 65 30 38 35 62 30 62 62 36 33 61 66 63 64 31 33 2e 65 78 65	C:\Users\user\Desktop\256 ec8f8 f67b59c5e085b0bb63afcd1 3.exe	success or wait	1	5250A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA082.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	5250A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5250A53	ReadFile

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	5250C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 6540 Parent PID: 6416

General

Start time:	19:10:10
Start date:	21/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp98F0.tmp'
Imagebase:	0xc00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp98F0.tmp	unknown	2	success or wait	1	C0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp98F0.tmp	unknown	1323	success or wait	1	C0ABD9	ReadFile

Analysis Process: conhost.exe PID: 6744 Parent PID: 6540

General

Start time:	19:10:12
Start date:	21/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6632 Parent PID: 6416

General

Start time:	19:10:12
Start date:	21/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpA082.tmp'
Imagebase:	0xc00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA082.tmp	unknown	2	success or wait	1	C0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA082.tmp	unknown	1311	success or wait	1	C0ABD9	ReadFile

Analysis Process: conhost.exe PID: 6764 Parent PID: 6632

General

Start time:	19:10:13
Start date:	21/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 256ec8f8f67b59c5e085b0bb63afcd13.exe PID: 6888 Parent PID: 968

General

Start time:	19:10:14
Start date:	21/02/2021
Path:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe 0
Imagebase:	0xda0000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
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: 00000007.00000002.707013030.0000000004471000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.707013030.0000000004471000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.707013030.0000000004471000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	722760AC	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	722760AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: dhcpmon.exe PID: 2460 Parent PID: 968

General

Start time:	19:10:14
Start date:	21/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x1c0000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
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: 00000008.00000002.717514074.0000000003B51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.717514074.0000000003B51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.717514074.0000000003B51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: dhcpmon.exe PID: 7160 Parent PID: 3424

General

Start time:	19:10:20
Start date:	21/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xdb0000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
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: 0000000A.00000002.730081391.00000000044D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.730081391.00000000044D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.730081391.00000000044D1000.00000004.00000001.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	722760AC	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	722760AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: 256ec8f8f67b59c5e085b0bb63afcd13.exe PID: 6260 Parent PID: 6888

General

Start time:	19:10:24
Start date:	21/02/2021
Path:	C:\Users\user\Desktop\256ec8f8f67b59c5e085b0bb63afcd13.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe00000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
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: 0000000B.00000002.721135661.0000000003471000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.721135661.0000000003471000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.719796822.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.719796822.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.719796822.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.721168712.0000000004471000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.721168712.0000000004471000.00000004.00000001.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	722760AC	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	722760AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6500 Parent PID: 2460

General

Start time:	19:10:25
Start date:	21/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb90000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
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: 0000000C.00000002.722378411.0000000003371000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.722378411.0000000003371000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.721387726.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.721387726.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.721387726.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.722411296.0000000004371000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.722411296.0000000004371000.00000004.00000001.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	722760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: dhcpmon.exe PID: 5748 Parent PID: 7160

General

Start time:	19:10:36
Start date:	21/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x810000
File size:	412672 bytes
MD5 hash:	0BBCC2E64E3EDF053ED4AF2C0BAFB0EB
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: 0000000E.00000002.742484463.0000000003FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.742484463.0000000003FB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.741098736.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.741098736.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.741098736.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.742370218.0000000002FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.742370218.0000000002FB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis