ID: 358272
Sample Name:
bbbe7872ea466446da60c4da50020cbb.exe
Cookbook: default.jbs
Time: 11:23:48
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

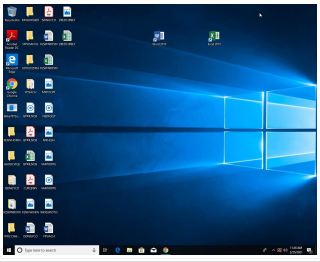
Analysis Report bbbe7872ea466446da60c4da50020cbb….

Overview

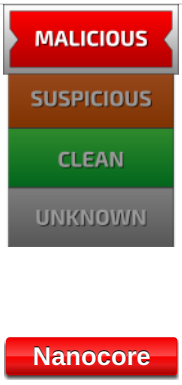
General Information

Sample Name:	bbbe7872ea466446da60c4da50020cbb.exe
Analysis ID:	358272
MD5:	88ef84e623f21af…
SHA1:	701339b101c76fa.
SHA256:	0095c39f2d6f62d..
Tags:	exe NanoCore nVpn RAT
Infos:	

Most interesting Screenshot:



Detection



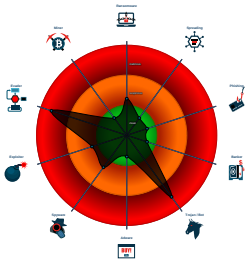
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- bbbe7872ea466446da60c4da50020cbb.exe (PID: 6780 cmdline: 'C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe' MD5: 88EF84E623F21AF8C30D3BBA321A7448)
  - bbbe7872ea466446da60c4da50020cbb.exe (PID: 6996 cmdline: C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe MD5: 88EF84E623F21AF8C30D3BBA321A7448)
    - schtasks.exe (PID: 7072 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7E95.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 7124 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp81B3.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- bbbe7872ea466446da60c4da50020cbb.exe (PID: 5620 cmdline: C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe 0 MD5: 88EF84E623F21AF8C30D3BBA321A7448)
  - bbbe7872ea466446da60c4da50020cbb.exe (PID: 348 cmdline: C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe MD5: 88EF84E623F21AF8C30D3BBA321A7448)
- dhcpmon.exe (PID: 5656 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 88EF84E623F21AF8C30D3BBA321A7448)
  - dhcpmon.exe (PID: 6240 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 88EF84E623F21AF8C30D3BBA321A7448)
  - dhcpmon.exe (PID: 6332 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 88EF84E623F21AF8C30D3BBA321A7448)
- dhcpmon.exe (PID: 6084 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 88EF84E623F21AF8C30D3BBA321A7448)
  - dhcpmon.exe (PID: 6340 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 88EF84E623F21AF8C30D3BBA321A7448)
- **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.org",
  "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
0000000C.00000002.375004523.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000002.375004523.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.375004523.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000E.00000002.381191346.0000000003D31000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.381191346.0000000003D3 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x49a5d:$a: NanoCore • 0x49ab6:$a: NanoCore • 0x49af3:$a: NanoCore • 0x49b6c:$a: NanoCore • 0x5d217:$a: NanoCore • 0x5d22c:$a: NanoCore • 0x5d261:$a: NanoCore • 0x76233:$a: NanoCore • 0x76248:$a: NanoCore • 0x7627d:$a: NanoCore • 0x49abf:$b: ClientPlugin • 0x49afc:$b: ClientPlugin • 0x4a3fa:$b: ClientPlugin • 0x4a407:$b: ClientPlugin • 0x5cfd3:$b: ClientPlugin • 0x5cfee:$b: ClientPlugin • 0x5d01e:$b: ClientPlugin • 0x5d235:$b: ClientPlugin • 0x5d26a:$b: ClientPlugin • 0x75fef:$b: ClientPlugin • 0x7600a:$b: ClientPlugin
Click to see the 53 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.dhcpmon.exe.40530dd.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x241a0:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x241cd:$x2: IClientNetworkHost
16.2.dhcpmon.exe.40530dd.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x241a0:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x2527b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x241ba:$s5: IClientLoggingHost
16.2.dhcpmon.exe.40530dd.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
14.2.dhcpmon.exe.2d53ac8.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
14.2.dhcpmon.exe.2d53ac8.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 131 entries				

Sigma Overview

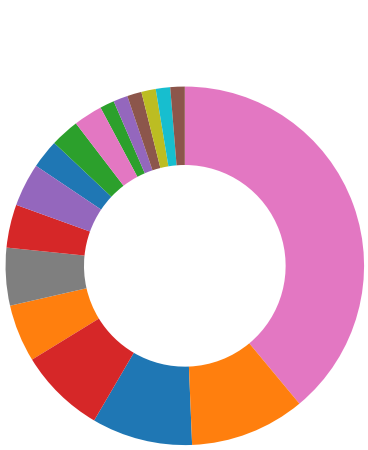
System Summary:

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



Click to jump to signature section

AV Detection:

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

Compliance:

- 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)
- .NET source code contains very large strings

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)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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:

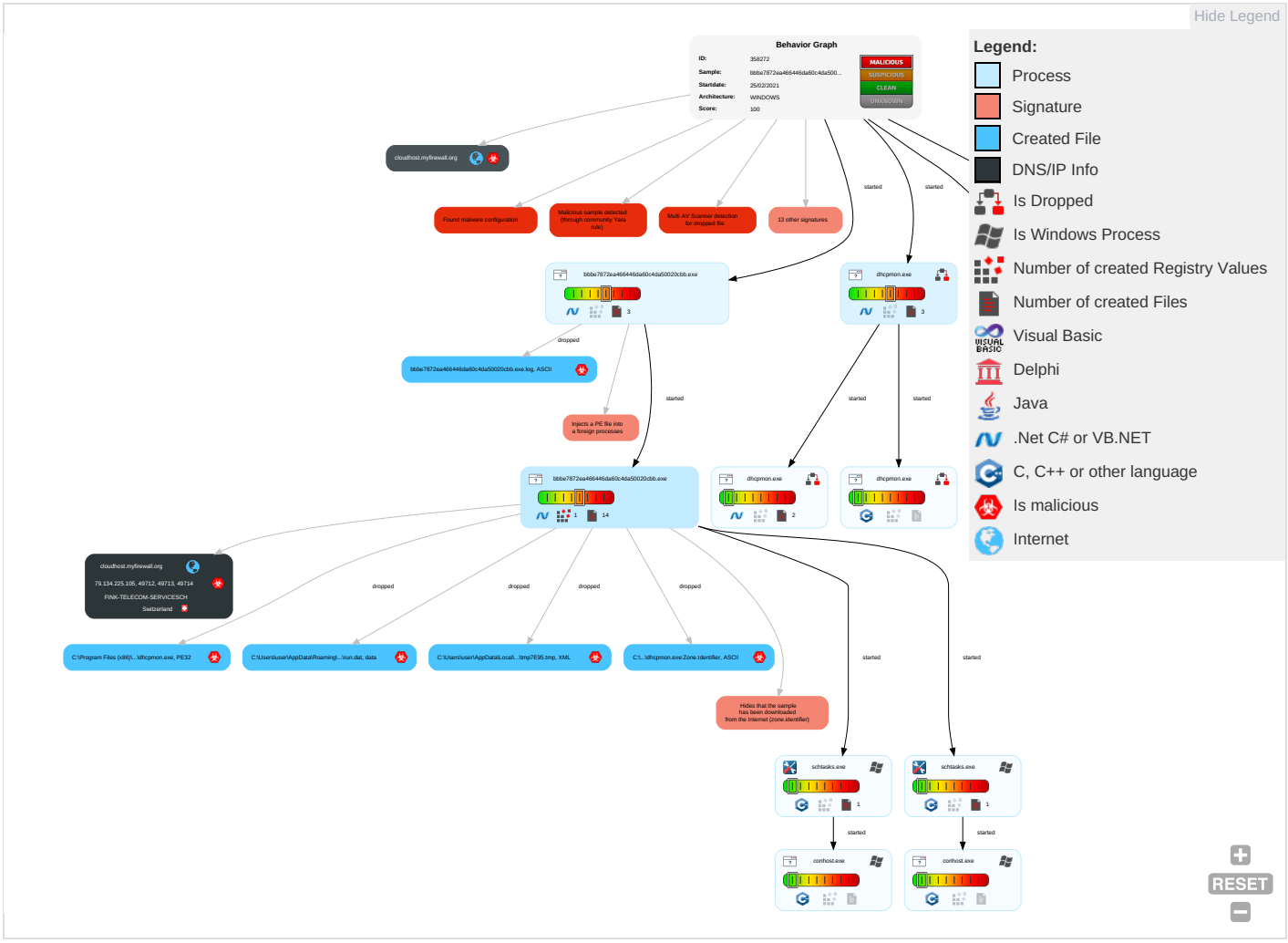
Detected Nanocore Rat

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 2 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	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	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	System Information Discovery 1 2	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 1	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

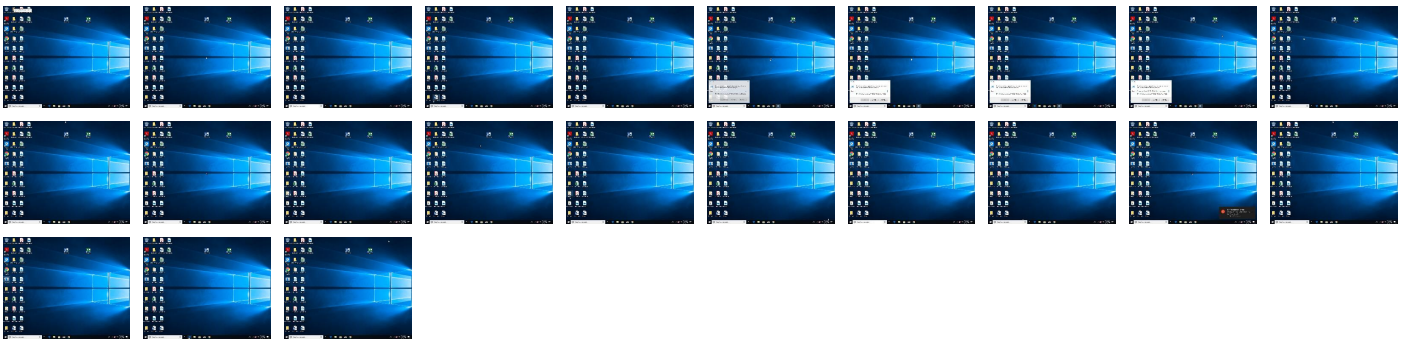
Behavior Graph



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
bbbe7872ea466446da60c4da50020cbb.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
bbbe7872ea466446da60c4da50020cbb.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.bbbe7872ea466446da60c4da50020cbb.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.bbbe7872ea466446da60c4da50020cbb.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.dhcpmon.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	0%	Avira URL Cloud	safe	
http://www.carterandcone.com&	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.carterandcone.comormD	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.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.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	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.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.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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	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.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.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.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	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.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/D	0%	Avira URL Cloud	safe	
http://www.gagalive.kr/livechat1.swf?chatroom=inchat-	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	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.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.carterandcone.comTCw	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/vvT	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	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 00000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.0000000005450000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.carterandcone.com&	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.329135863.00000000051A7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 00000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 00000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 00000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comormD	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.328197714.00000000051A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 00000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.329135863.00000000051A7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.343834467.0000000002D51000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 00000A.00000002.364695909.0000000002DF1000.00000004.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.367072310.0000000002F6100 0.00000004.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.379503086.0000000002831000.00000004.00000001.sdmp	false		high
http://www.carterandcone.com.	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.328197714.00000000051A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

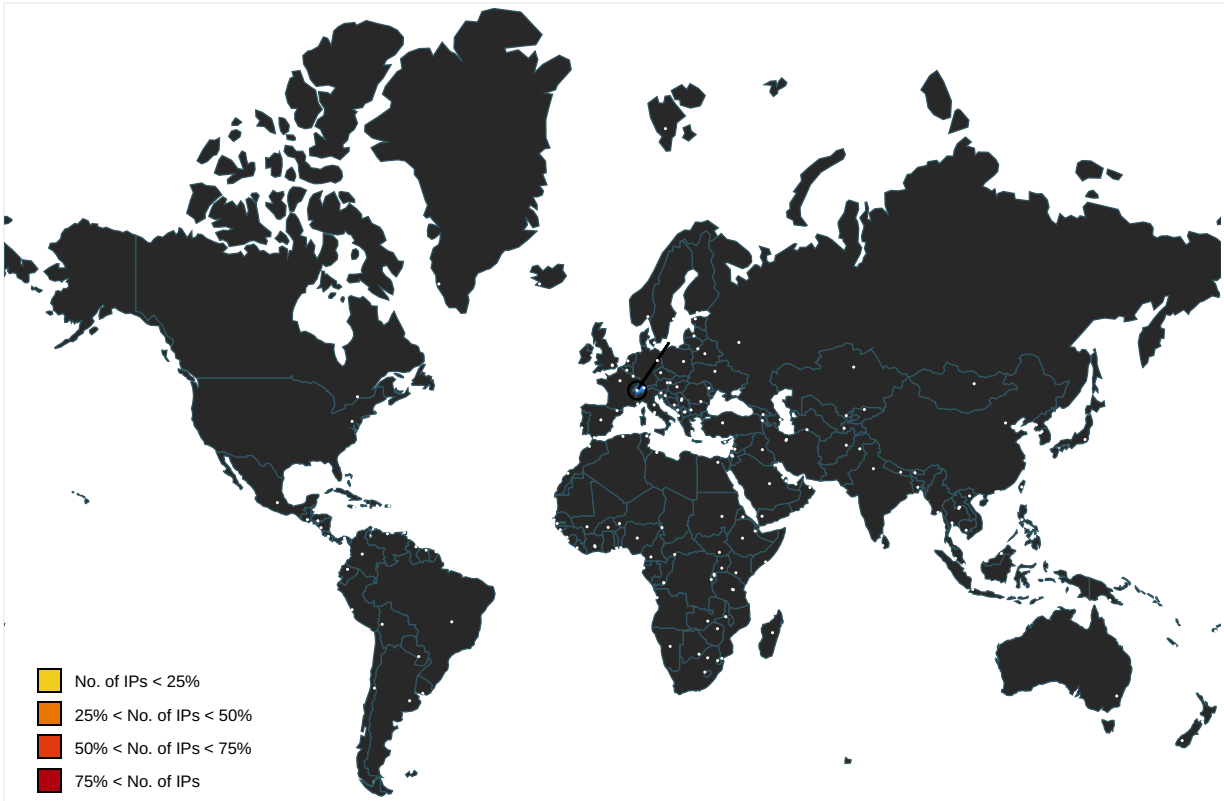
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.329603375.00000000051A8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.330244134.00000000051DD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/(	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.3296 03375.00000000051A8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.3480 97971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466 446da60c4da50020cbb.exe, 00000 00A.00000002.367125363.0000000 005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.0000 0002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcp mon.exe, 0000000F.00000002.382 568285.0000000004EB0000.000000 02.00000001.sdmp	false		high
http://www.sandoll.co.kr	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.3480 97971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466 446da60c4da50020cbb.exe, 00000 00A.00000002.367125363.0000000 005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.0000 0002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcp mon.exe, 0000000F.00000002.382 568285.0000000004EB0000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.3480 97971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466 446da60c4da50020cbb.exe, 00000 00A.00000002.367125363.0000000 005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.0000 0002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcp mon.exe, 0000000F.00000002.382 568285.0000000004EB0000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.3480 97971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466 446da60c4da50020cbb.exe, 00000 00A.00000002.367125363.0000000 005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.0000 0002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcp mon.exe, 0000000F.00000002.382 568285.0000000004EB0000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.3281 97714.00000000051A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.3480 97971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466 446da60c4da50020cbb.exe, 00000 00A.00000002.367125363.0000000 005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.0000 0002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcp mon.exe, 0000000F.00000002.382 568285.0000000004EB0000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schooldb.inchat.kro.kr/	dhcpmon.exe, dhcpmon.exe, 0000 000E.00000002.378594437.000000 0000502000.00000002.00020000.sdmp, dhcpmon.exe, 0000000F.000 00000.371490717.0000000000420 00.00000002.00020000.sdmp, dhc pmon.exe, 00000010.00000002.39 0560823.00000000008F2000.00000 002.00020000.sdmp, bbbe7872ea4 66446da60c4da50020cbb.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.334789389.00000000051D5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://inchat.kro.kr	dhcpmon.exe, dhcpmon.exe, 0000000E.00000002.378594437.0000000000502000.00000002.00020000.sdmp, dhcpmon.exe, 0000000F.00000000.371490717.0000000000042000.00000002.00020000.sdmp, dhcpmon.exe, 00000010.00000002.390560823.00000000008F2000.00000002.00020000.sdmp, bbbe7872ea466446da60c4da50020cbb.exe	false		high
http://www.fontbureau.com/designers/cabarga.htmlo	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.333166545.00000000051D5000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comTC	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.328197714.00000000051A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnp	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.328197714.00000000051A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/D	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.329603375.00000000051A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gagalive.kr/livechat1.swf?chatroom=inchat-	dhcpmon.exe, dhcpmon.exe, 0000000E.00000002.378594437.0000000000502000.00000002.00020000.sdmp, dhcpmon.exe, 0000000F.00000000.371490717.0000000000042000.00000002.00020000.sdmp, dhcpmon.exe, 00000010.00000002.390560823.00000000008F2000.00000002.00020000.sdmp, bbbe7872ea466446da60c4da50020cbb.exe	false	• Avira URL Cloud: safe	unknown
http://en.w	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.325630674.00000000051A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.000000000545000 0.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.327774459.00000000051AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.0000000005450000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.0000000005450000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.332711004.00000000051D5000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.0000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.0000000005450000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.333166545.00000000051D5000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comTCw	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.328197714.00000000051A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.0000000005450000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/vvT	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000003.329603375.00000000051A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	bbbe7872ea466446da60c4da50020cbb.exe, 00000000.00000002.348097971.00000000063B2000.00000004.00000001.sdmp, bbbe7872ea466446da60c4da50020cbb.exe, 0000000A.00000002.367125363.0000000005320000.00000002.00000001.sdmp, dhcpmon.exe, 0000000B.00000002.370057992.0000000005450000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.382568285.0000000004EB0000.00000002.00000001.sdmp	false		high

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:	358272
Start date:	25.02.2021
Start time:	11:23:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bbbe7872ea466446da60c4da50020cbb.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:	37
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@20/8@20/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.6%) • Quality average: 61.9% • Quality standard deviation: 18.7%
HCA Information:	• Successful, ratio: 86% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.103.5.186, 104.43.139.144, 204.79.197.200, 13.107.21.200, 23.218.209.198, 104.42.151.234, 92.122.145.220, 52.255.188.83, 51.104.144.132, 67.26.75.254, 8.253.207.120, 8.248.147.254, 67.27.158.254, 8.248.137.254, 52.155.217.156, 51.103.5.159, 20.54.26.129, 92.122.213.247, 92.122.213.194, 104.43.193.48, 51.104.139.180, 184.30.20.56 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:24:42	API Interceptor	911x Sleep call for process: bbbe7872ea466446da60c4da50020cbb.exe modified
11:24:47	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe" s>$(Arg0)
11:24:48	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
11:24:49	API Interceptor	2x Sleep call for process: dhcpmon.exe modified
11:24:49	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.105	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	
	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	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	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	cp573oYDUX.exe	Get hash	malicious	Browse	• 79.134.225.43
	Y5XyMnx8Ng.exe	Get hash	malicious	Browse	• 79.134.225.43
	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 79.134.225.43
	xF7GogN7tM.exe	Get hash	malicious	Browse	• 79.134.225.120

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TZgGVyMJYF.exe	Get hash	malicious	Browse	• 79.134.225.74
	ilpbALnKbE.exe	Get hash	malicious	Browse	• 79.134.225.103
	Documents.exe	Get hash	malicious	Browse	• 79.134.225.87
	SWcNyi2YBj.exe	Get hash	malicious	Browse	• 79.134.225.103
	Confirmation Transfer Note Ref Number0002636.exe	Get hash	malicious	Browse	• 79.134.225.8
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 79.134.225.43
	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	WxTm2cWLHF.exe	Get hash	malicious	Browse	• 79.134.225.71
	Payment Confirmation.exe	Get hash	malicious	Browse	• 79.134.225.30
	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	487424
Entropy (8bit):	7.585377119878555
Encrypted:	false
SSDEEP:	12288:13Wp0pFZhvpNkMtT4vH2PEe4nU7YTRwiQSBuDG9RDQ1Ln:1ZFZDWocvHwt4bqDMDQF
MD5:	88EF84E623F21AF8C30D3BBA321A7448
SHA1:	701339B101C76FA1BA159C66B48EF2F9B6D73AA8
SHA-256:	0095C39F2D6F62DEA9FD6D066DECAB6F0A7ACAB87829F659EFD01BC1D2564BD0
SHA-512:	2441191F7FE76BFEF584960ED21EC576DD36D0FD37882F77A91A0FC05921A7B459E030FCBC4E3A3207F55BA9D8992CDD69F20A87C1837FF2EAC13C1F89D1603
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6`.....P..f..... .....@.. ..... ..@.....O..... ..... ..H.....text...4d... ...f..... ..`.rsrc.....h.....@..@.reloc..... .....n.....@..B.....H.....lE.....:...I.....0.....(....(.....(.....o....*.....(.....(.....(!.....("......(#....*N..(....o....($....*&..(%. ...*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~.....(0.....,!r.. .p.....(1...o2...s3.....~.....+..*.0.....

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

Process:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.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**

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\bbbe7872ea466446da60c4da50020cbb.exe.log	
Process:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.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\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.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):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.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\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp7E95.tmp	
Process:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1325
Entropy (8bit):	5.142681781286418
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0VxuDxtn:cbk4oL600QydbQxIYODOLedq3iij
MD5:	84A099124F6C7EE51E18E71DC7BC3A9B
SHA1:	1711144C438CBDF89365DB7FA6321956BC973CF7
SHA-256:	8239178C04A3BA7C0A51E29EA046C53C7DFD6434CA19F053730578CEB231B4F9
SHA-512:	E3653310916ADF9C0A96AAC010900B7E2A7B7156651A06B53E75110A212A1C9A6489CE58E9D856B8A4DD473612D91C760D5855B9E3200496B3D4204DF4AA91AF
Malicious:	**true**
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\tmp81B3.tmp	
Process:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.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\bbbe7872ea466446da60c4da50020cbb.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:hn:h
MD5:	D31129909503FD8FFBD27BEC609FAEFB
SHA1:	31E23DEAE7A4A3318FEDE87058CD39880371C5A6
SHA-256:	A8BD14E933B3B91C59B72BBE9F0CE37D00BFD53DC4E41A838E4488F8B1C4FDC4
SHA-512:	C3CC657202070CF423E811054FBB0C4DC48BC2545DD7DC0DD2FD4D392F17985C71D920E918FD145F2DEE0C85691CD4F43F664B13A0E07B279DC1A63E7D57AB8
Malicious:	**true**
Preview:	..E....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.443732754068415
Encrypted:	false
SSDEEP:	3:oNN2+WHAuK1T95RbXVQHLNn:oNN2RguuhbXVQrNn
MD5:	1305CC0074A93B66ED5F48F9F5525B0A
SHA1:	FF47387DBEDCF1D78859AE5E69D68087E9D001B8
SHA-256:	2683F197FE07E73150EFC619A6D18BD2D459B37B243B109A350F697E50033E38
SHA-512:	54CAD3A91F06B1651FEF9F3B34ED4DCC4445D36D4E77E8F61A8C74049ADD13CBFDB8F246CFDE78CB634170234D04C30726B5E4956955FDCEE7AC5760E1A888C
Malicious:	false
Preview:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.585377119878555

General

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:	bbbe7872ea466446da60c4da50020cbb.exe
File size:	487424
MD5:	88ef84e623f21af8c30d3bba321a7448
SHA1:	701339b101c76fa1ba159c66b48ef2f9b6d73aa8
SHA256:	0095c39f2d6f62dea9fd6d066decab6f0a7acab87829f659efd01bc1d2564bd0
SHA512:	2441191f7fe76bfef584960ed21ec576dd36d0fd37882f77a91a0fc05921a7b459e030fcbc4e3a3207f55ba9d8992cdd69f20a87c1837ff2eac13c1f89d16035
SSDEEP:	12288:13Wp0pFZhvpNkMtT4vH2PEe4nU7YTRwiQSBuDG9RDQ1Ln:1ZFZDWocvHwt4bqDMDQF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6`.....P..f..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47842e
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:	0x6036DFEC [Wed Feb 24 23:23:24 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x783dc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7a000	0x5dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7c000	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	0x76434	0x76600	False	0.81248968783	data	7.59845021391	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x5dc	0x600	False	0.43359375	data	4.18581494296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	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	0x7a090	0x34c	data		
RT_MANIFEST	0x7a3ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

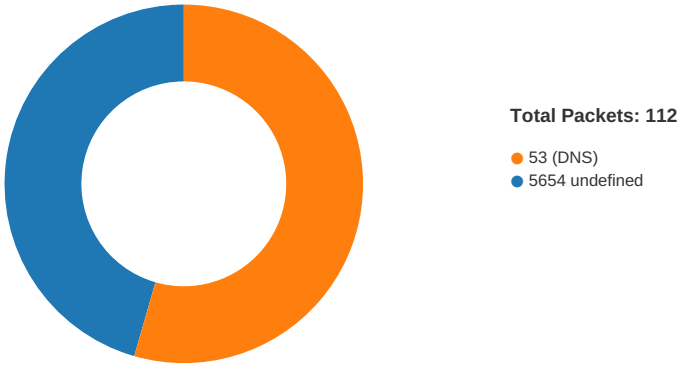
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 - 2021
Assembly Version	1.0.0.0
InternalName	SystemLazyDebugView.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ASM PS
ProductVersion	1.0.0.0
FileDescription	ASM PS
OriginalFilename	SystemLazyDebugView.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:24:48.626800060 CET	49712	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:24:48.709671974 CET	5654	49712	79.134.225.105	192.168.2.6
Feb 25, 2021 11:24:49.325844049 CET	49712	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:24:49.410424948 CET	5654	49712	79.134.225.105	192.168.2.6
Feb 25, 2021 11:24:50.025794983 CET	49712	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:24:50.109920979 CET	5654	49712	79.134.225.105	192.168.2.6
Feb 25, 2021 11:24:54.695738077 CET	49713	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:24:54.783087969 CET	5654	49713	79.134.225.105	192.168.2.6
Feb 25, 2021 11:24:55.354371071 CET	49713	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:24:55.439676046 CET	5654	49713	79.134.225.105	192.168.2.6
Feb 25, 2021 11:24:56.058144093 CET	49713	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:24:56.145593882 CET	5654	49713	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:00.273941040 CET	49714	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:00.358505964 CET	5654	49714	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:00.870687962 CET	49714	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:00.955174923 CET	5654	49714	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:01.464282036 CET	49714	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:01.547135115 CET	5654	49714	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:05.998193979 CET	49721	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:06.080715895 CET	5654	49721	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:06.589694977 CET	49721	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:06.673861980 CET	5654	49721	79.134.225.105	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:25:07.183506966 CET	49721	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:07.266280890 CET	5654	49721	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:11.364681959 CET	49727	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:11.450200081 CET	5654	49727	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:12.121423006 CET	49727	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:12.209835052 CET	5654	49727	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:12.824589014 CET	49727	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:12.910170078 CET	5654	49727	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:17.076725006 CET	49730	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:17.161436081 CET	5654	49730	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:17.668745041 CET	49730	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:17.751597881 CET	5654	49730	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:18.262532949 CET	49730	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:18.347594023 CET	5654	49730	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:22.442135096 CET	49731	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:22.529938936 CET	5654	49731	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:23.044122934 CET	49731	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:23.132652044 CET	5654	49731	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:23.637950897 CET	49731	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:23.730770111 CET	5654	49731	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:27.997536898 CET	49738	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:28.080324888 CET	5654	49738	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:28.591954947 CET	49738	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:28.677618027 CET	5654	49738	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:29.202150106 CET	49738	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:29.284926891 CET	5654	49738	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:33.562685013 CET	49745	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:33.648861885 CET	5654	49745	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:34.201298952 CET	49745	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:34.294214010 CET	5654	49745	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:34.904462099 CET	49745	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:34.989918947 CET	5654	49745	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:39.131872892 CET	49752	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:39.214664936 CET	5654	49752	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:39.717439890 CET	49752	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:39.800367117 CET	5654	49752	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:40.311438084 CET	49752	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:40.394157887 CET	5654	49752	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:44.567759037 CET	49753	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:44.653165102 CET	5654	49753	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:45.155433893 CET	49753	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:45.240783930 CET	5654	49753	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:45.749188900 CET	49753	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:45.835782051 CET	5654	49753	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:49.973664045 CET	49757	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:50.060617924 CET	5654	49757	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:50.562046051 CET	49757	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:25:50.651330948 CET	5654	49757	79.134.225.105	192.168.2.6
Feb 25, 2021 11:25:51.155955076 CET	49757	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:07.282320023 CET	49761	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:07.372164011 CET	5654	49761	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:07.876277924 CET	49761	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:07.958929062 CET	5654	49761	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:08.469770908 CET	49761	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:08.552668095 CET	5654	49761	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:12.692601919 CET	49764	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:12.779438972 CET	5654	49764	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:13.282622099 CET	49764	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:13.368633032 CET	5654	49764	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:13.876403093 CET	49764	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:13.963768005 CET	5654	49764	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:18.590110064 CET	49765	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:18.677874088 CET	5654	49765	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:19.189440966 CET	49765	5654	192.168.2.6	79.134.225.105

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:26:19.277095079 CET	5654	49765	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:19.783225060 CET	49765	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:19.868992090 CET	5654	49765	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:24.321764946 CET	49766	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:24.409323931 CET	5654	49766	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:24.928036928 CET	49766	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:25.013566017 CET	5654	49766	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:25.518033028 CET	49766	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:25.603816032 CET	5654	49766	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:29.753073931 CET	49768	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:29.837347031 CET	5654	49768	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:30.354100943 CET	49768	5654	192.168.2.6	79.134.225.105
Feb 25, 2021 11:26:30.436645985 CET	5654	49768	79.134.225.105	192.168.2.6
Feb 25, 2021 11:26:30.947804928 CET	49768	5654	192.168.2.6	79.134.225.105

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:24:27.117582083 CET	57725	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:27.166593075 CET	53	57725	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:28.176310062 CET	49283	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:28.217499971 CET	58377	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:28.225069046 CET	53	49283	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:28.269035101 CET	53	58377	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:29.046103001 CET	55074	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:29.118208885 CET	53	55074	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:29.214934111 CET	54513	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:29.264540911 CET	53	54513	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:30.449815035 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:30.501537085 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:32.090500116 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:32.160540104 CET	53	63791	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:33.270864010 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:33.319513083 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:34.359849930 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:34.411431074 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:48.212694883 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:48.389832020 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 11:24:54.637378931 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:24:54.694610119 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:00.210314035 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:00.270603895 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:03.047249079 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:03.095995903 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:04.005820990 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:04.054773092 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:04.948786020 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:04.997585058 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:05.491166115 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:05.542964935 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:05.925417900 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:05.988379002 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:06.118753910 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:06.167573929 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:07.061675072 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:07.110531092 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:08.066205025 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:08.115267038 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:08.901803970 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:08.962486029 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:10.411164999 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:10.468545914 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:11.305735111 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:11.363370895 CET	53	50055	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:25:13.473772049 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:13.523927927 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:14.458923101 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:14.508641005 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:17.018151045 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:17.075424910 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:22.383959055 CET	49694	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:22.440958977 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:22.454272032 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:22.506934881 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:25.711648941 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:25.768949032 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:26.315239906 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:26.366815090 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:27.118741989 CET	62116	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:27.126820087 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:27.175472021 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:27.175956011 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:27.606359005 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:27.663378954 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:27.907069921 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:27.952208042 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:27.964279890 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:28.019773006 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:28.168005943 CET	51818	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:28.225503922 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:28.942802906 CET	56628	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:29.002837896 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:30.171575069 CET	60778	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:30.232163906 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:31.825973988 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:31.874722958 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:33.121190071 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:33.173006058 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:33.444616079 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:33.494067907 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:33.657452106 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:33.707140923 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:36.012670040 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:36.075216055 CET	53	56129	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:39.068284988 CET	58177	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:39.117019892 CET	53	58177	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:44.506081104 CET	50700	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:44.566046000 CET	53	50700	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:45.987143993 CET	54069	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:46.037607908 CET	53	54069	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:47.105782032 CET	61178	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:47.158185005 CET	53	61178	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:48.100619078 CET	57017	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:48.150759935 CET	53	57017	8.8.8.8	192.168.2.6
Feb 25, 2021 11:25:49.913017988 CET	56327	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:25:49.971278906 CET	53	56327	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:04.542124987 CET	50243	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:04.593692064 CET	53	50243	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:04.987422943 CET	62055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:05.052566051 CET	53	62055	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:07.228221893 CET	61249	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:07.280585051 CET	53	61249	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:08.916820049 CET	65252	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:08.977189064 CET	53	65252	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:12.625998974 CET	64367	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:12.690673113 CET	53	64367	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:18.522969007 CET	55066	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:18.585977077 CET	53	55066	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:26:24.260216951 CET	60211	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:24.320557117 CET	53	60211	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:28.934892893 CET	56570	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:28.983767033 CET	53	56570	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:29.690567017 CET	58454	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:29.752105951 CET	53	58454	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:35.151140928 CET	55180	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:35.208693981 CET	53	55180	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:40.576133966 CET	58721	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:40.637666941 CET	53	58721	8.8.8.8	192.168.2.6
Feb 25, 2021 11:26:45.918656111 CET	57691	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:26:45.976176023 CET	53	57691	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:24:48.212694883 CET	192.168.2.6	8.8.8.8	0xeff6	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:24:54.637378931 CET	192.168.2.6	8.8.8.8	0x104c	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:00.210314035 CET	192.168.2.6	8.8.8.8	0xc159	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:05.925417900 CET	192.168.2.6	8.8.8.8	0x556a	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:11.305735111 CET	192.168.2.6	8.8.8.8	0xeb5	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:17.018151045 CET	192.168.2.6	8.8.8.8	0x3637	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:22.383959055 CET	192.168.2.6	8.8.8.8	0x15a1	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:27.907069921 CET	192.168.2.6	8.8.8.8	0x8fb3	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:33.444616079 CET	192.168.2.6	8.8.8.8	0x9128	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:39.068284988 CET	192.168.2.6	8.8.8.8	0xc65d	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:44.506081104 CET	192.168.2.6	8.8.8.8	0xbda7	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:49.913017988 CET	192.168.2.6	8.8.8.8	0x1d2f	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:07.228221893 CET	192.168.2.6	8.8.8.8	0xafc0	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:12.625998974 CET	192.168.2.6	8.8.8.8	0xb43d	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:18.522969007 CET	192.168.2.6	8.8.8.8	0xd2af	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:24.260216951 CET	192.168.2.6	8.8.8.8	0xd4ec	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:29.690567017 CET	192.168.2.6	8.8.8.8	0xd408	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:35.151140928 CET	192.168.2.6	8.8.8.8	0x1c71	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:40.576133966 CET	192.168.2.6	8.8.8.8	0x1429	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:45.918656111 CET	192.168.2.6	8.8.8.8	0x7f8d	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

DNS Answers

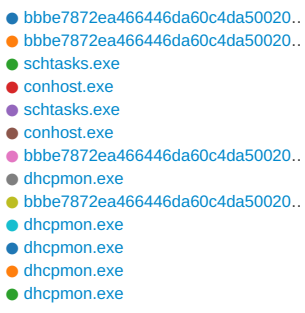
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:24:48.389832020 CET	8.8.8.8	192.168.2.6	0xeff6	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:24:54.694610119 CET	8.8.8.8	192.168.2.6	0x104c	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:00.270603895 CET	8.8.8.8	192.168.2.6	0xc159	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:05.988379002 CET	8.8.8.8	192.168.2.6	0x556a	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)

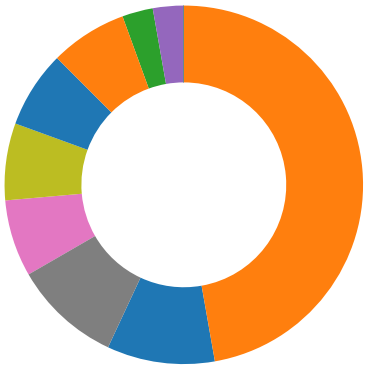
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:25:11.363370895 CET	8.8.8.8	192.168.2.6	0xeb5	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:17.075424910 CET	8.8.8.8	192.168.2.6	0x3637	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:22.440958977 CET	8.8.8.8	192.168.2.6	0x15a1	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:27.964279890 CET	8.8.8.8	192.168.2.6	0x8fb3	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:33.494067907 CET	8.8.8.8	192.168.2.6	0x9128	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:39.117019892 CET	8.8.8.8	192.168.2.6	0xc65d	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:44.566046000 CET	8.8.8.8	192.168.2.6	0xbda7	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:25:49.971278906 CET	8.8.8.8	192.168.2.6	0x1d2f	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:07.280585051 CET	8.8.8.8	192.168.2.6	0xafc0	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:12.690673113 CET	8.8.8.8	192.168.2.6	0xb43d	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:18.585977077 CET	8.8.8.8	192.168.2.6	0xd2af	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:24.320557117 CET	8.8.8.8	192.168.2.6	0xd4ec	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:29.752105951 CET	8.8.8.8	192.168.2.6	0xd408	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:35.208693981 CET	8.8.8.8	192.168.2.6	0x1c71	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:40.637666941 CET	8.8.8.8	192.168.2.6	0x1429	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 25, 2021 11:26:45.976176023 CET	8.8.8.8	192.168.2.6	0x7f8d	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: bbbe7872ea466446da60c4da50020cbb.exe PID: 6780 Parent PID: 5892

General

Start time:	11:24:36
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe'
Imagebase:	0x590000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.343834467.0000000002D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.344108345.0000000003D51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.344108345.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.344108345.0000000003D51000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\bbbe7872ea466446da60c4da50020cbb.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	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\bbbe7872ea466446da60c4da50020cbb.exe.log	unknown	664	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: bbbe7872ea466446da60c4da50020cbb.exe PID: 6996 Parent PID: 6780

General

Start time:	11:24:43
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
Imagebase:	0x620000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
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: 00000004.00000002.592467577.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.592467577.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.592467577.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.597683140.0000000003D07000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.597683140.0000000003D07000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4F907A1	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	4F9089B	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	4F907A1	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	4F90B20	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	4F90B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7E95.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4F90D1C	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	4F9089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp81B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4F90D1C	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	4F907A1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4F907A1	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	72FB60AC	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	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7E95.tmp	success or wait	1	110BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp81B3.tmp	success or wait	1	110BF0E	DeleteFileW
C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe:Zone.Identifier	success or wait	1	4F9114D	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	c9 18 45 02 c3 d9 d8 48	..E....H	success or wait	1	4F90A53	WriteFile
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 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 ec df 36 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 66 07 00 00 08 00 00 00 00 00 00 2e 84 07 00 00 20 00 00 00 a0 07 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 00 e0 07 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....6`.......... ....P..f.............. ....@.. ....@................	success or wait	4	4F90B20	CopyFileW
C:\Program Files (x86)\DHCP Monitor\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	4F90B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7E95.tmp	unknown	1325	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.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	4F90A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	62	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 62 62 62 65 37 38 37 32 65 61 34 36 36 34 34 36 64 61 36 30 63 34 64 61 35 30 30 32 30 63 62 62 2e 65 78 65	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe	success or wait	1	4F90A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp81B3.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 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	4F90A53	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4F90A53	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	4F90C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 7072 Parent PID: 6996

General

Start time:	11:24:45
Start date:	25/02/2021
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\tmp7E95.tmp'
Imagebase:	0x340000
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\tmp7E95.tmp	unknown	2	success or wait	1	34AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7E95.tmp	unknown	1326	success or wait	1	34ABD9	ReadFile

Analysis Process: conhost.exe PID: 7080 Parent PID: 7072

General

Start time:	11:24:45
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000

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: 7124 Parent PID: 6996

General

Start time:	11:24:46
Start date:	25/02/2021
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\tmp81B3.tmp'
Imagebase:	0x340000
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\tmp81B3.tmp	unknown	2	success or wait	1	34AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp81B3.tmp	unknown	1311	success or wait	1	34ABD9	ReadFile

Analysis Process: conhost.exe PID: 7132 Parent PID: 7124

General

Start time:	11:24:46
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: bbbe7872ea466446da60c4da50020cbb.exe PID: 5620 Parent PID: 936

General

Start time:	11:24:48
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe 0
Imagebase:	0x720000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
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.00000002.365772164.0000000003DF1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.365772164.0000000003DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.365772164.0000000003DF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.364695909.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security
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	72FB60AC	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	72FB60AC	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 5656 Parent PID: 936

General

Start time:	11:24:48
Start date:	25/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x720000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
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: 0000000B.00000002.367529312.0000000003F61000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.367529312.0000000003F61000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.367529312.0000000003F61000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.367072310.0000000002F61000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	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	72FA34A7	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	664	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: bbbe7872ea466446da60c4da50020cbb.exe PID: 348 Parent PID: 5620

General

Start time:	11:24:49
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\bbbe7872ea466446da60c4da50020cbb.exe
Imagebase:	0x790000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
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: 0000000C.00000002.375004523.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.375004523.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.375004523.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.377624667.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.377624667.0000000002DA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.377737091.0000000003DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.377737091.0000000003DA1000.00000004.00000001.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	72FB60AC	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	72FB60AC	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6240 Parent PID: 5656

General

Start time:	11:24:52
Start date:	25/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x1f0000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6332 Parent PID: 5656

General

Start time:	11:24:54
Start date:	25/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x500000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
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.00000002.381191346.0000000003D31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.381191346.0000000003D31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.381077094.0000000002D31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.381077094.0000000002D31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.378479336.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.378479336.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.378479336.0000000000402000.00000040.00000001.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	72FB60AC	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	72FB60AC	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6084 Parent PID: 3440

General

Start time:	11:24:58
Start date:	25/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x40000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.379503086.0000000002831000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.380529240.0000000003831000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.380529240.0000000003831000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.380529240.0000000003831000.00000004.00000001.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	72FB60AC	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	72FB60AC	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown

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	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6340 Parent PID: 6084

General

Start time:	11:24:59
Start date:	25/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x8f0000
File size:	487424 bytes
MD5 hash:	88EF84E623F21AF8C30D3BBA321A7448
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: 00000010.00000002.391674013.0000000004001000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.391674013.0000000004001000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.390499078.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.390499078.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.390499078.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.391635582.0000000003001000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.391635582.0000000003001000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis