ID: 356808
Sample Name:
e92b274943f4a3a557881ee0dd57772d.exe
Cookbook: default.jbs
Time: 17:06:18
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report e92b274943f4a3a557881ee0dd57772d.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: NanoCore 5
Yara Overview 6
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Compliance: 7
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Data Obfuscation: 8
Boot Survival: 8
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
Contacted IPs 18
Public 18
Private 19
General Information 19
Simulations 20
Behavior and APIs 20
Joe Sandbox View / Context 20
IPs 20
Domains 21
ASN 21
JA3 Fingerprints 21
Dropped Files 21
Created / dropped Files 22
Static File Info 24

General 24
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 25
Data Directories 26
Sections 27
Resources 27
Imports 27
Version Infos 27
Network Behavior 27
Network Port Distribution 27
TCP Packets 28
UDP Packets 29
DNS Queries 31
DNS Answers 32
Code Manipulations 33
Statistics 33
Behavior 33
System Behavior 33
Analysis Process: e92b274943f4a3a557881ee0dd57772d.exe PID: 5900 Parent PID: 5628 33
General 33
File Activities 33
File Created 34
File Written 34
File Read 34
Analysis Process: e92b274943f4a3a557881ee0dd57772d.exe PID: 6108 Parent PID: 5900 34
General 34
File Activities 35
File Created 35
File Deleted 36
File Written 36
File Read 37
Registry Activities 38
Key Value Created 38
Analysis Process: schtasks.exe PID: 2336 Parent PID: 6108 38
General 38
File Activities 38
File Read 38
Analysis Process: conhost.exe PID: 4012 Parent PID: 2336 38
General 38
Analysis Process: schtasks.exe PID: 2880 Parent PID: 6108 39
General 39
File Activities 39
File Read 39
Analysis Process: conhost.exe PID: 4860 Parent PID: 2880 39
General 39
Analysis Process: e92b274943f4a3a557881ee0dd57772d.exe PID: 6200 Parent PID: 904 39
General 39
File Activities 40
File Created 40
File Read 40
Analysis Process: dhcpmon.exe PID: 6296 Parent PID: 904 40
General 40
File Activities 41
File Created 41
File Written 41
File Read 42
Analysis Process: e92b274943f4a3a557881ee0dd57772d.exe PID: 6460 Parent PID: 6200 42
General 42
File Activities 42
File Created 42
File Read 42
Analysis Process: dhcpmon.exe PID: 6468 Parent PID: 6296 43
General 43
File Activities 43
File Created 43
File Read 43
Analysis Process: dhcpmon.exe PID: 6720 Parent PID: 3472 43
General 43
File Activities 44
File Created 44
File Read 44

Analysis Process: dhcpmon.exe PID: 7024 Parent PID: 6720 44
General 44
Analysis Process: backgroundTaskHost.exe PID: 7024 Parent PID: 792 45
General 45
Disassembly 45
Code Analysis 45

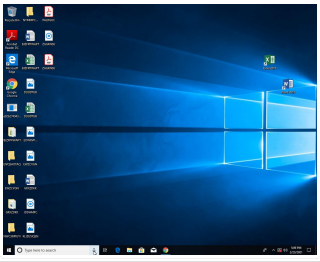
Analysis Report e92b274943f4a3a557881ee0dd57772d.e…

Overview

General Information

Sample Name:	e92b274943f4a3a557881ee0dd57772d.exe
Analysis ID:	356808
MD5:	1f2b71c462d73dc..
SHA1:	98957c96b7c2dd..
SHA256:	c6e001729b8abc..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

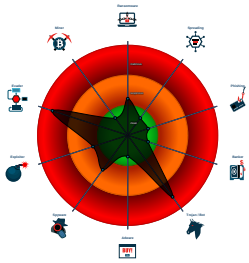
Nanocore

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…
- 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…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- e92b274943f4a3a557881ee0dd57772d.exe (PID: 5900 cmdline: 'C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe' MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
  - e92b274943f4a3a557881ee0dd57772d.exe (PID: 6108 cmdline: C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
    - schtasks.exe (PID: 2336 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp22EF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2880 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp266B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- e92b274943f4a3a557881ee0dd57772d.exe (PID: 6200 cmdline: C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe 0 MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
  - e92b274943f4a3a557881ee0dd57772d.exe (PID: 6460 cmdline: C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
- dhcpmon.exe (PID: 6296 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
  - dhcpmon.exe (PID: 6468 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
- dhcpmon.exe (PID: 6720 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
  - dhcpmon.exe (PID: 7024 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 1F2B71C462D73DCDCC69A707A18C38D6)
  - backgroundTaskHost.exe (PID: 7024 cmdline: 'C:\Windows\system32\backgroundTaskHost.exe' -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca MD5: B7FC4A29431D4F795BBAB1FB182B759A)
- **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.00000002.289277143.0000000002BF1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000014.00000002.310042790.00000000033F1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.252323083.0000000002BC7000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000009.00000002.275215575.0000000002FD4000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000009.00000002.275177741.0000000002FB1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 52 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
12.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
12.2.dhcpmon.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
12.2.dhcpmon.exe.3c430dd.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x241a0:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x241cd:$x2: IClientNetworkHost
Click to see the 124 entries				

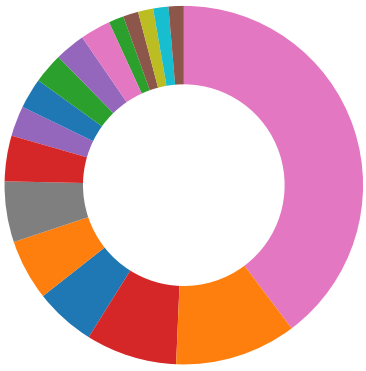
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

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

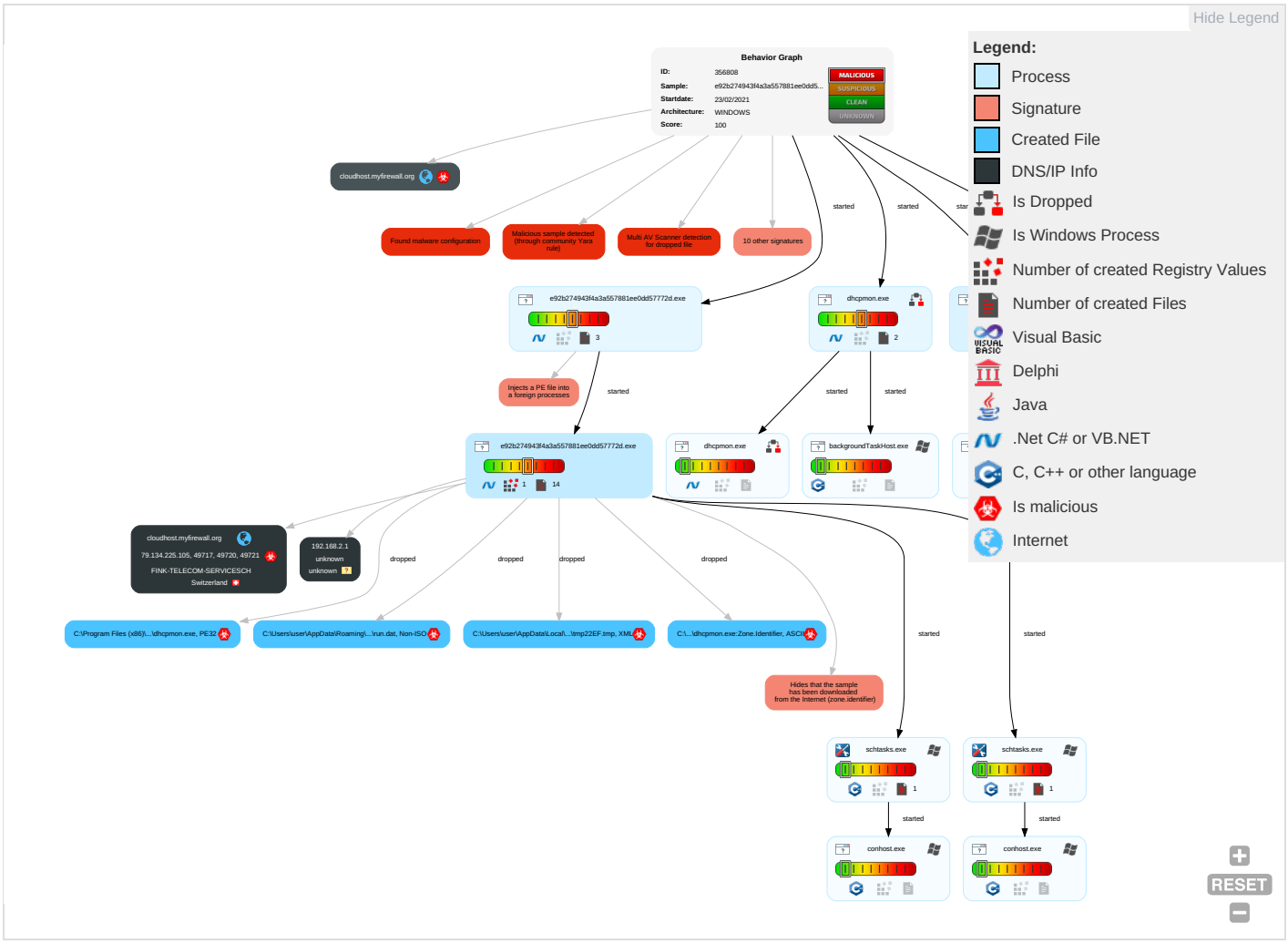
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect

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	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	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)	Logon Script (Windows)	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)	Process Injection 1 1 2	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	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

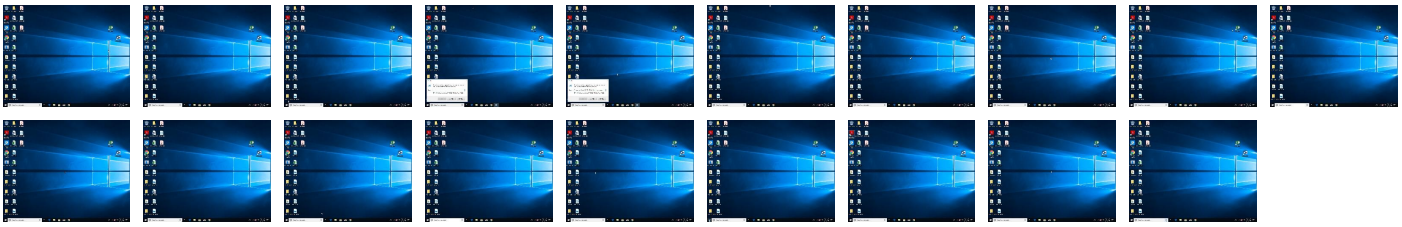
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	10%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.e92b274943f4a3a557881ee0dd57772d.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.e92b274943f4a3a557881ee0dd57772d.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
cloudhost.myfirewall.org	1%	Virustotal		Browse
cloudhost.myfirewall.org	0%	Avira URL Cloud	safe	
http://qunect.com/download/QuNect.exe	0%	Virustotal		Browse
http://qunect.com/download/QuNect.exe	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/j4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/O	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/04x	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnU	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.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.jiyu-kobo.co.jp/-4	0%	Avira URL Cloud	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.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/cn0	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comporH	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/c4	0%	Avira URL Cloud	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.founder.com.cn/cn/i	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krnta	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.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	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://qunect.com/download/QuNect.exeMOperation	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnu-h	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasva04x	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/T4$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.0000000 2.00000001.sdmp, e92b274943f4a 3a557881ee0dd57772d.exe, 00000 009.00000002.278284760.0000000 005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.0000 0002.279293564.00000000059E000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000010.00000002.294 768587.0000000004F30000.000000 02.00000001.sdmp	false		high
http://www.fontbureau.com	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.0000000 2.00000001.sdmp, e92b274943f4a 3a557881ee0dd57772d.exe, 00000 009.00000002.278284760.0000000 005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.0000 0002.279293564.00000000059E000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000010.00000002.294 768587.0000000004F30000.000000 02.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.0000000 2.00000001.sdmp, e92b274943f4a 3a557881ee0dd57772d.exe, 00000 009.00000002.278284760.0000000 005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.0000 0002.279293564.00000000059E000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000010.00000002.294 768587.0000000004F30000.000000 02.00000001.sdmp	false		high
http://qunect.com/download/QuNect.exe	dhcpmon.exe, dhcpmon.exe, 0000 000C.00000002.287680615.000000 0000492000.00000002.00020000.sdmp, dhcpmon.exe, 00000010.000 00000.282951821.00000000002820 00.00000002.00020000.sdmp, dhc pmon.exe, 00000014.00000000.28 8641273.0000000000D42000.00000 002.00020000.sdmp, e92b274943f 4a3a557881ee0dd57772d.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.250488584.0000000005020000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/j4	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.237262965.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/a-e	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.237262965.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/O	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.237262965.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/04x	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.237262965.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnU	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.235501924.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false		high

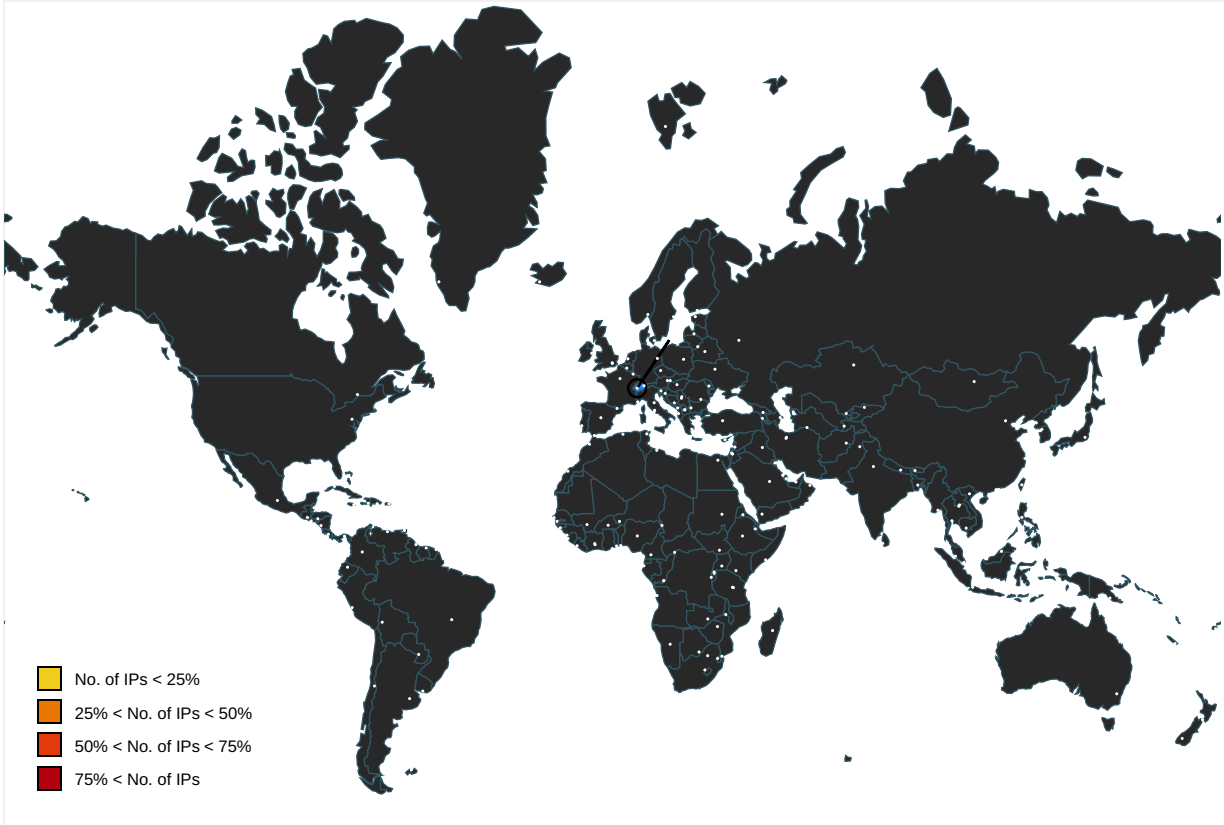
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.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	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.252323083.0000000002BC7000.00000004.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.275215575.0000000002FD4000.00000004.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275680850.00000000033D6000.00000004.00000001.sdmp, dhcpmon.exe, 00000010.00000002.292745387.0000000002A27000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.233760280.000000000503B000.00000004.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/-4	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.237262965.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn0	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.2354 91079.000000000505D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.2555 51391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false		high
http://www.sajatypeworks.comporH	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.2337 17864.000000000503E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.2372 62965.0000000005024000.00000004.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/c4	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.237262965.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://validator.w3.org/check?uri=referer	e92b274943f4a3a557881ee0dd57772d.exe	false		high
http://www.fontbureau.com/designers8	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersg#	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.240286022.0000000005029000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/i	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.235685065.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krnta	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.234803629.0000000005029000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.233921994.000000000503B000.00000004.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://qunect.com/download/QuNect.exeMOperation	e92b274943f4a3a557881ee0dd57772d.exe	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnu-h	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.235491079.000000000505D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000002.255551391.0000000005110000.00000002.00000001.sdmp, e92b274943f4a3a557881ee0dd57772d.exe, 00000009.00000002.278284760.0000000005590000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.279293564.00000000059E0000.00000002.00000001.sdmp, dhcpmon.exe, 00000010.00000002.294768587.0000000004F30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comx	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.233865303.000000000503B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comasva04x	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.250488584.0000000005020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/T4$	e92b274943f4a3a557881ee0dd57772d.exe, 00000000.00000003.237262965.0000000005024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356808
Start date:	23.02.2021
Start time:	17:06:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e92b274943f4a3a557881ee0dd57772d.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:	32
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@19/8@22/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.7% (good quality ratio 1.4%) • Quality average: 46.2% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 51.103.5.186, 13.64.90.137, 204.79.197.200, 13.107.21.200, 93.184.220.29, 51.11.168.160, 168.61.161.212, 23.211.6.115, 40.88.32.150, 104.42.151.234, 184.30.24.56, 51.103.5.159, 51.104.139.180, 92.122.213.247, 92.122.213.194, 20.54.26.129, 84.53.167.113 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:07:17	API Interceptor	913x Sleep call for process: e92b274943f4a3a557881ee0dd57772d.exe modified
17:07:23	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe" s>$(Arg0)
17:07:23	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
17:07:25	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:07:26	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.105	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	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	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
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	Solicitud de oferta 6100003768.exe	Get hash	malicious	Browse	• 79.134.225.96
	Nrfgylra.exe	Get hash	malicious	Browse	• 79.134.225.96
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	Form pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	Quotation 3342688.exe	Get hash	malicious	Browse	• 79.134.225.120
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 79.134.225.76

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	475648
Entropy (8bit):	7.633075553718302
Encrypted:	false
SSDEEP:	12288:KDWVp7lNYUvq2gFgkeu0cNOYVAKe7dE9jGEiuk:KiV57Yr99eu0cN3VC7vEil
MD5:	1F2B71C462D73DCDCC69A707A18C38D6
SHA1:	98957C96B7C2DD066B6C5108F8DED53983427472
SHA-256:	C6E001729B8ABC3D321756D6964E1A84148F19004F03606953EBBA32081F4C75
SHA-512:	EE9033D27B384894BC73BFC9AB21ECE48D3FF9CE858A99C29B10F9F687DE0201AFBD238B6141ABC6D44775979AC368D4E843B8F78B910751F187F87F2857C8F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....4`.....P..,.....K... ...`....@.. ....@.....hK..O....`..... ..... ..H.....text....+... ...,..... ..`.rsrc.....`.....@..@.reloc..... .....@.....@..B.....K.....H.....?.....n.....R.....0.....(....(.....(.....o....*.....(.....(.....(!.....("....(#....*N..(....og...($. ...*&..(%....*.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\e92b274943f4a3a557881ee0dd57772d.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\e92b274943f4a3a557881ee0dd57772d.exe.log	
Process:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\e92b274943f4a3a557881ee0dd57772d.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp22EF.tmp	
Process:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1323
Entropy (8bit):	5.1600199834185245
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Pmxtn:cbk4oL600QydbQxIYODOLedq3Smj
MD5:	A2656079C3A26D530BF27B9B65082EB8
SHA1:	8B4B44848C52291110A41283EACEE9922B6B5DD2
SHA-256:	3CE09B678463F0BB81EF3CC3DD814BC99937D3F9D2203CE3CAAB188D5FAD603E
SHA-512:	20B281B387315EDF7624B37906DC74B9016FF2C41C6612C373C33F6C97076A6B78A532FED66A078BF99E5FD64346119038EBAD0AD4AB2FB1B1EC5F27E7B31E4
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\tmp266B.tmp	
Process:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.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\e92b274943f4a3a557881ee0dd57772d.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:a1ft:a/
MD5:	27205FFD95E8C21E294722F6C7C90F87
SHA1:	AE76805E7334FDB1C3D0AD94DE3E37BF98732DE4
SHA-256:	B3FAE43AD48058B592FCE99E646420CECCBF1F62296B6571A51BFD9102EA059B
SHA-512:	1B10F5AAD92C94689BCA4C13D9455DBD4E33E38225A1FCC32E2BB9BCECA4B8C61518F8C14A0782E522F862B291A4CE3970117E9813F705E9D5DB62AD8B12B86
Malicious:	**true**
Preview:	./.`..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.556297888280896
Encrypted:	false
SSDEEP:	3:oNUWJRWAii2FS8lVyILN:oNNJAAiHFnl7
MD5:	3597821A0D92E1F7F1C2EE61421DE72B
SHA1:	D15AB9D668CE9589CABF2B508791D845EA04C68C
SHA-256:	D881E5C2A38DC4DBE74A711776BD7EB83E777593FEACAAA8BEED9A9520256CFC
SHA-512:	1FDC4AE5A9E2FC2BF6A48D5D6AB09933F796E567E362E965C83888301FDC80CF53570D008ED2157CC462749E832411A3030E319B015AA135836445B80F581118
Malicious:	false
Preview:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.633075553718302
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:	e92b274943f4a3a557881ee0dd57772d.exe
File size:	475648
MD5:	1f2b71c462d73dcdcc69a707a18c38d6
SHA1:	98957c96b7c2dd066b6c5108f8ded53983427472
SHA256:	c6e001729b8abc3d321756d6964e1a84148f19004f03606953ebba32081f4c75
SHA512:	ee9033d27b384894bc73bfc9ab21ece48d3ff9ce858a99c29b10f9f687de0201afbd238b6141abc6d44775979ac368d4e843b8f78b910751f187f87f2857c8f8
SSDEEP:	12288:KDWVp7lNYUvq2gFgkeu0cNOYVAKe7dE9jGEiuk:KiV57Yr99eu0cN3VC7vEil
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....4`.....P..,.....K... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x474bba

General

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:	0x6034EC9E [Tue Feb 23 11:53:02 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74b68	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x76000	0x10fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x78000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
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	0x72bc0	0x72c00	False	0.835452410131	data	7.64910376893	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x10fc	0x1200	False	0.377387152778	data	4.91259584588	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	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	0x76090	0x32e	data		
RT_MANIFEST	0x763d0	0xd25	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	1.0.0.23
InternalName	Filters.exe
FileVersion	1.0.0.23
CompanyName	
LegalTrademarks	
Comments	
ProductName	QuNectRestore
ProductVersion	1.0.0.23
FileDescription	QuNectRestore
OriginalFilename	Filters.exe

Network Behavior

Network Port Distribution

Total Packets: 98

- 53 (DNS)
- 5654 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:07:24.317401886 CET	49717	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:24.402925968 CET	5654	49717	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:25.006032944 CET	49717	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:25.170547009 CET	5654	49717	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:25.802982092 CET	49717	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:25.890747070 CET	5654	49717	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:30.196755886 CET	49720	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:30.279649019 CET	5654	49720	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:30.803371906 CET	49720	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:30.888102055 CET	5654	49720	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:31.506556988 CET	49720	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:31.591274977 CET	5654	49720	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:35.747231960 CET	49721	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:35.831572056 CET	5654	49721	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:36.506983995 CET	49721	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:36.589525938 CET	5654	49721	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:37.194564104 CET	49721	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:37.279087067 CET	5654	49721	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:41.383832932 CET	49724	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:41.467339039 CET	5654	49724	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:42.007436991 CET	49724	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:42.091211081 CET	5654	49724	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:42.695390940 CET	49724	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:42.777978897 CET	5654	49724	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:47.502105951 CET	49725	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:47.587483883 CET	5654	49725	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:48.195631027 CET	49725	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:48.280992031 CET	5654	49725	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:48.804977894 CET	49725	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:48.903510094 CET	5654	49725	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:53.099952936 CET	49726	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:53.185305119 CET	5654	49726	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:53.696875095 CET	49726	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:53.782341957 CET	5654	49726	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:54.305444002 CET	49726	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:54.390938044 CET	5654	49726	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:58.496613026 CET	49728	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:58.579344988 CET	5654	49728	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:59.086997986 CET	49728	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:59.172306061 CET	5654	49728	79.134.225.105	192.168.2.5
Feb 23, 2021 17:07:59.680921078 CET	49728	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:07:59.765491009 CET	5654	49728	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:04.214276075 CET	49731	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:04.297036886 CET	5654	49731	79.134.225.105	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:08:04.806471109 CET	49731	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:04.892066956 CET	5654	49731	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:05.477663040 CET	49731	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:05.562105894 CET	5654	49731	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:09.662631035 CET	49732	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:09.748166084 CET	5654	49732	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:10.362611055 CET	49732	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:10.450221062 CET	5654	49732	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:11.009932041 CET	49732	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:11.095531940 CET	5654	49732	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:15.200858116 CET	49735	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:15.285886049 CET	5654	49735	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:15.900957108 CET	49735	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:15.983403921 CET	5654	49735	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:16.510380030 CET	49735	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:16.592907906 CET	5654	49735	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:20.703866005 CET	49736	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:20.791032076 CET	5654	49736	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:21.401786089 CET	49736	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:21.488744020 CET	5654	49736	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:22.010874033 CET	49736	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:22.096328974 CET	5654	49736	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:26.488413095 CET	49737	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:26.570949078 CET	5654	49737	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:27.214370966 CET	49737	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:27.298923969 CET	5654	49737	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:27.882488012 CET	49737	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:27.967346907 CET	5654	49737	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:32.081837893 CET	49738	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:32.167021036 CET	5654	49738	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:32.709744930 CET	49738	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:32.794991016 CET	5654	49738	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:33.308701992 CET	49738	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:33.393233061 CET	5654	49738	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:37.513951063 CET	49740	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:37.599510908 CET	5654	49740	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:38.105928898 CET	49740	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:38.193403006 CET	5654	49740	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:38.699738026 CET	49740	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:38.786367893 CET	5654	49740	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:42.932596922 CET	49741	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:43.016801119 CET	5654	49741	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:43.528386116 CET	49741	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:43.610882998 CET	5654	49741	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:44.122071981 CET	49741	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:44.204689026 CET	5654	49741	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:48.332449913 CET	49745	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:48.425596952 CET	5654	49745	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:48.935069084 CET	49745	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:49.022025108 CET	5654	49745	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:49.528836966 CET	49745	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:49.619158983 CET	5654	49745	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:53.743664026 CET	49746	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:53.830708981 CET	5654	49746	79.134.225.105	192.168.2.5
Feb 23, 2021 17:08:54.341633081 CET	49746	5654	192.168.2.5	79.134.225.105
Feb 23, 2021 17:08:54.424118042 CET	5654	49746	79.134.225.105	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:07:01.966917992 CET	52212	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:02.010678053 CET	53	52704	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:02.019895077 CET	53	52212	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:02.493860006 CET	54302	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:07:02.544358969 CET	53	54302	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:02.673930883 CET	53784	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:02.731071949 CET	53	53784	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:03.031584978 CET	65307	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:03.083000898 CET	53	65307	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:03.093507051 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:03.142283916 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:03.245066881 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:03.296475887 CET	53	62060	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:04.191267967 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:04.243364096 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:05.222963095 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:05.272953033 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:06.924113989 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:06.973278046 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:07.422972918 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:07.481489897 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:08.339463949 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:08.390849113 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:09.774693966 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:09.831759930 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:10.627614021 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:10.684992075 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:11.850918055 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:11.902892113 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:14.212620974 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:14.264101982 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:15.498347998 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:15.547302961 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:16.382819891 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:16.436593056 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:23.839442015 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:23.905378103 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:27.270549059 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:27.335716963 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:30.128424883 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:30.195499897 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:35.678299904 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:35.744441986 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:39.990731955 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:40.041691065 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:41.318376064 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:41.382150888 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:47.434134007 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:47.496967077 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:53.038328886 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:53.097796917 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:57.724330902 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:57.775765896 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 17:07:58.442466021 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:07:58.494002104 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:00.102087975 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:00.154416084 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:04.155479908 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:04.213018894 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:09.601368904 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:09.661525011 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:11.137090921 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:11.195926905 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:15.129806995 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:15.187225103 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:20.635152102 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:20.699871063 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:26.388084888 CET	59261	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:08:26.483036041 CET	53	59261	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:32.018039942 CET	57151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:32.080794096 CET	53	57151	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:32.346096992 CET	59413	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:32.414536953 CET	53	59413	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:37.451399088 CET	60516	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:37.508657932 CET	53	60516	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:42.865860939 CET	51649	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:42.930672884 CET	53	51649	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:43.815403938 CET	65086	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:43.876554012 CET	53	65086	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:45.763406992 CET	56432	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:45.815440893 CET	53	56432	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:47.436276913 CET	52929	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:47.493521929 CET	53	52929	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:48.270625114 CET	64317	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:48.329891920 CET	53	64317	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:53.683684111 CET	61004	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:53.740900993 CET	53	61004	8.8.8.8	192.168.2.5
Feb 23, 2021 17:08:59.079591990 CET	56895	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:08:59.144479036 CET	53	56895	8.8.8.8	192.168.2.5
Feb 23, 2021 17:09:04.518706083 CET	62372	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:09:04.586355925 CET	53	62372	8.8.8.8	192.168.2.5
Feb 23, 2021 17:09:10.028256893 CET	61515	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:09:10.088375092 CET	53	61515	8.8.8.8	192.168.2.5
Feb 23, 2021 17:09:15.767822981 CET	56675	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:09:15.830482006 CET	53	56675	8.8.8.8	192.168.2.5
Feb 23, 2021 17:09:21.130548954 CET	57172	53	192.168.2.5	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:07:23.839442015 CET	192.168.2.5	8.8.8.8	0xb8c3	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:30.128424883 CET	192.168.2.5	8.8.8.8	0xc4f5	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:35.678299904 CET	192.168.2.5	8.8.8.8	0xa15b	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:41.318376064 CET	192.168.2.5	8.8.8.8	0x9c0a	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:47.434134007 CET	192.168.2.5	8.8.8.8	0xce56	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.038328886 CET	192.168.2.5	8.8.8.8	0x7248	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:58.442466021 CET	192.168.2.5	8.8.8.8	0x8b2	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:04.155479908 CET	192.168.2.5	8.8.8.8	0x7c47	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:09.601368904 CET	192.168.2.5	8.8.8.8	0xa2dd	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:15.129806995 CET	192.168.2.5	8.8.8.8	0x1d5d	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:20.635152102 CET	192.168.2.5	8.8.8.8	0x5eee	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.388084888 CET	192.168.2.5	8.8.8.8	0xbd45	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:32.018039942 CET	192.168.2.5	8.8.8.8	0x965a	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:37.451399088 CET	192.168.2.5	8.8.8.8	0xd55e	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:42.865860939 CET	192.168.2.5	8.8.8.8	0x8c7	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:48.270625114 CET	192.168.2.5	8.8.8.8	0x26f9	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:53.683684111 CET	192.168.2.5	8.8.8.8	0x9280	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:59.079591990 CET	192.168.2.5	8.8.8.8	0xee40	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:09:04.518706083 CET	192.168.2.5	8.8.8.8	0xd1c9	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:10.028256893 CET	192.168.2.5	8.8.8.8	0x6e8a	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:15.767822981 CET	192.168.2.5	8.8.8.8	0xdc2b	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:21.130548954 CET	192.168.2.5	8.8.8.8	0xd499	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

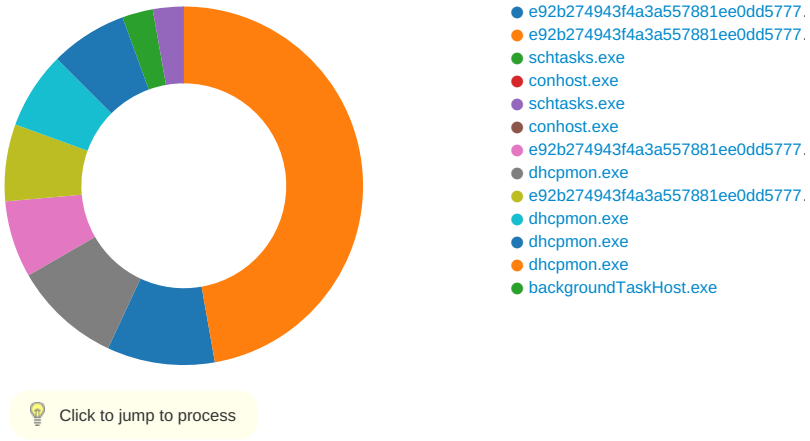
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:07:23.905378103 CET	8.8.8.8	192.168.2.5	0xb8c3	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:30.195499897 CET	8.8.8.8	192.168.2.5	0xc4f5	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:35.744441986 CET	8.8.8.8	192.168.2.5	0xa15b	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:41.382150888 CET	8.8.8.8	192.168.2.5	0x9c0a	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:47.496967077 CET	8.8.8.8	192.168.2.5	0xce56	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.097796917 CET	8.8.8.8	192.168.2.5	0x7248	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:58.494002104 CET	8.8.8.8	192.168.2.5	0x8b2	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:04.213018894 CET	8.8.8.8	192.168.2.5	0x7c47	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:09.661525011 CET	8.8.8.8	192.168.2.5	0xa2dd	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:15.187225103 CET	8.8.8.8	192.168.2.5	0x1d5d	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:20.699871063 CET	8.8.8.8	192.168.2.5	0x5eee	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.483036041 CET	8.8.8.8	192.168.2.5	0xbd45	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:32.080794096 CET	8.8.8.8	192.168.2.5	0x965a	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:37.508657932 CET	8.8.8.8	192.168.2.5	0xd55e	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:42.930672884 CET	8.8.8.8	192.168.2.5	0x8c7	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:48.329891920 CET	8.8.8.8	192.168.2.5	0x26f9	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:53.740900993 CET	8.8.8.8	192.168.2.5	0x9280	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:59.144479036 CET	8.8.8.8	192.168.2.5	0xee40	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:04.586355925 CET	8.8.8.8	192.168.2.5	0xd1c9	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:10.088375092 CET	8.8.8.8	192.168.2.5	0x6e8a	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:15.830482006 CET	8.8.8.8	192.168.2.5	0xdc2b	No error (0)	cloudhost.myfirewall.org		79.134.225.105	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: e92b274943f4a3a557881ee0dd57772d.exe PID: 5900 Parent PID: 5628

General

Start time:	17:07:10
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe'
Imagebase:	0x4c0000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
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: 00000000.00000002.252323083.0000000002BC7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.252271147.0000000002BA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.252610124.0000000003BA1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.252610124.0000000003BA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.252610124.0000000003BA1000.00000004.00000001.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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\e92b274943f4a3a557881ee0dd57772d.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	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\e92b274943f4a3a557881ee0dd57772d.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: e92b274943f4a3a557881ee0dd57772d.exe PID: 6108 Parent PID: 5900

General

Start time:	17:07:18
Start date:	23/02/2021

Path:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
Imagebase:	0x7ff797770000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.499071538.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.499071538.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.499071538.0000000000402000.00000040.00000001.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	72B860AC	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	72B860AC	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	4E007A1	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	4E0089B	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	4E007A1	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	4E00B20	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	4E00B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp22EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4E00D1C	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	4E0089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp266B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4E00D1C	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4E007A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4E007A1	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	72B860AC	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	72B860AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp22EF.tmp	success or wait	1	CFBF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp266B.tmp	success or wait	1	CFBF0E	DeleteFileW
C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe:Zone.Identifier	success or wait	1	4E0114D	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	c4 a9 2f 89 60 d8 d8 48	../.`..H	success or wait	1	4E00A53	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 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 9e ec 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 2c 07 00 00 14 00 00 00 00 00 00 ba 4b 07 00 00 20 00 00 00 60 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 a0 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....4`.......... ....P..,...........K... ...`....@.. ....@................	success or wait	4	4E00B20	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	4E00B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp22EF.tmp	unknown	1323	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	4E00A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	60	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 65 39 32 62 32 37 34 39 34 33 66 34 61 33 61 35 35 37 38 38 31 65 65 30 64 64 35 37 37 37 32 64 2e 65 78 65	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe	success or wait	1	4E00A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp266B.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	4E00A53	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4E00A53	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	4E00C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 2336 Parent PID: 6108

General

Start time:	17:07:20
Start date:	23/02/2021
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\tmp22EF.tmp'
Imagebase:	0xad0000
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\tmp22EF.tmp	unknown	2	success or wait	1	ADAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp22EF.tmp	unknown	1324	success or wait	1	ADABD9	ReadFile

Analysis Process: conhost.exe PID: 4012 Parent PID: 2336

General

Start time:	17:07:20
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000

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: 2880 Parent PID: 6108

General

Start time:	17:07:21
Start date:	23/02/2021
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\tmp266B.tmp'
Imagebase:	0xad0000
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\tmp266B.tmp	unknown	2	success or wait	1	ADAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp266B.tmp	unknown	1311	success or wait	1	ADABD9	ReadFile

Analysis Process: conhost.exe PID: 4860 Parent PID: 2880

General

Start time:	17:07:21
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: e92b274943f4a3a557881ee0dd57772d.exe PID: 6200 Parent PID: 904

General

Start time:	17:07:23
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe 0
Imagebase:	0x8c0000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
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: 00000009.00000002.275215575.0000000002FD4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.275177741.0000000002FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.275575320.0000000003FB1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.275575320.0000000003FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.275575320.0000000003FB1000.00000004.00000001.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	72B860AC	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	72B860AC	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6296 Parent PID: 904

General

Start time:	17:07:23
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xd10000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
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: 0000000A.00000002.275680850.00000000033D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.275574869.00000000033B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.276093432.00000000043B1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.276093432.00000000043B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.276093432.00000000043B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 10%, 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	72B860AC	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	72B860AC	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	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: e92b274943f4a3a557881ee0dd57772d.exe PID: 6460 Parent PID: 6200

General

Start time:	17:07:28
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\e92b274943f4a3a557881ee0dd57772d.exe
Imagebase:	0x850000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.290065986.0000000003EF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.290065986.0000000003EF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.289889933.0000000002EF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.287315536.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.287315536.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.287315536.0000000000402000.00000040.00000001.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	72B860AC	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	72B860AC	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6468 Parent PID: 6296

General

Start time:	17:07:28
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x490000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.289277143.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.289384974.0000000003BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.289384974.0000000003BF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.287530922.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.287530922.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.287530922.0000000000402000.00000040.00000001.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	72B860AC	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	72B860AC	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6720 Parent PID: 3472

General

Start time:	17:07:33
Start date:	23/02/2021

Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x280000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
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: 00000010.00000002.292745387.0000000002A27000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.293020224.0000000003A01000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.293020224.0000000003A01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.293020224.0000000003A01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.292697027.0000000002A01000.00000004.00000001.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	72B860AC	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	72B860AC	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: dhcpmon.exe PID: 7024 Parent PID: 6720

General

Start time:	17:07:36
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xd40000
File size:	475648 bytes
MD5 hash:	1F2B71C462D73DCDCC69A707A18C38D6
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: 00000014.00000002.310042790.00000000033F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.304832264.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.304832264.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.304832264.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.310443660.00000000043F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.310443660.00000000043F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: backgroundTaskHost.exe PID: 7024 Parent PID: 792

General

Start time:	17:09:01
Start date:	23/02/2021
Path:	C:\Windows\System32\backgroundTaskHost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\backgroundTaskHost.exe' -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca
Imagebase:	0x7ff64e5e0000
File size:	19352 bytes
MD5 hash:	B7FC4A29431D4F795BBAB1FB182B759A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis