ID: 357566
Sample Name:
m72OvSF7e5.exe
Cookbook: default.jbs
Time: 18:38:56
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

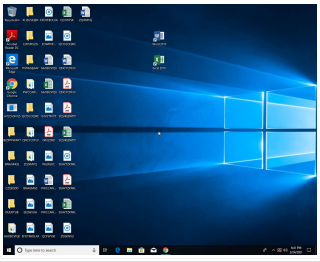
Analysis Report m72OvSF7e5.exe

Overview

General Information

Sample Name:	m72OvSF7e5.exe
Analysis ID:	357566
MD5:	8c596990203f7d1.
SHA1:	bcabae5c0b3ca8..
SHA256:	a98a739b9ab7b0..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

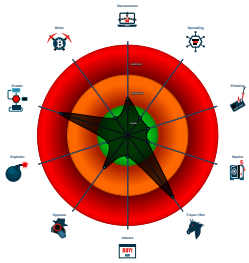
Nanocore

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…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- m72OvSF7e5.exe (PID: 6316 cmdline: 'C:\Users\user\Desktop\m72OvSF7e5.exe' MD5: 8C596990203F7D15651498FDBA84B5F3)
  - schtasks.exe (PID: 7104 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWdTBYiTWyTud' /XML 'C:\Users\user\AppData\Local\Temp\tmp79E0.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - m72OvSF7e5.exe (PID: 5808 cmdline: {path} MD5: 8C596990203F7D15651498FDBA84B5F3)
    - schtasks.exe (PID: 5404 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp84A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6412 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpE27.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- m72OvSF7e5.exe (PID: 6620 cmdline: C:\Users\user\Desktop\m72OvSF7e5.exe 0 MD5: 8C596990203F7D15651498FDBA84B5F3)
  - schtasks.exe (PID: 3276 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWdTBYiTWyTud' /XML 'C:\Users\user\AppData\Local\Temp\tmpF7E9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - m72OvSF7e5.exe (PID: 6096 cmdline: {path} MD5: 8C596990203F7D15651498FDBA84B5F3)
- dhcpmon.exe (PID: 4608 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 8C596990203F7D15651498FDBA84B5F3)
- dhcpmon.exe (PID: 404 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 8C596990203F7D15651498FDBA84B5F3)
  - schtasks.exe (PID: 2144 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWdTBYiTWyTud' /XML 'C:\Users\user\AppData\Local\Temp\tmp2CE4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6984 cmdline: {path} MD5: 8C596990203F7D15651498FDBA84B5F3)
  - dhcpmon.exe (PID: 5724 cmdline: {path} MD5: 8C596990203F7D15651498FDBA84B5F3)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "92421eeb-c456-44c2-ab8d-5a66d7e5ab97",
  "Group": "Company",
  "Domain1": "194.5.98.202",
  "Domain2": "",
  "Port": 4488,
  "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": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "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
0000001C.00000002.427245821.0000000003DA9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001C.00000002.427245821.0000000003DA9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x4356d:$a: NanoCore • 0x435c6:$a: NanoCore • 0x43603:$a: NanoCore • 0x4367c:$a: NanoCore • 0x56d27:$a: NanoCore • 0x56d3c:$a: NanoCore • 0x56d71:$a: NanoCore • 0x6fceb:$a: NanoCore • 0x6fd00:$a: NanoCore • 0x6fd35:$a: NanoCore • 0x435cf:$b: ClientPlugin • 0x4360c:$b: ClientPlugin • 0x43f0a:$b: ClientPlugin • 0x43f17:$b: ClientPlugin • 0x56ae3:$b: ClientPlugin • 0x56afe:$b: ClientPlugin • 0x56b2e:$b: ClientPlugin • 0x56d45:$b: ClientPlugin • 0x56d7a:$b: ClientPlugin • 0x6faa7:$b: ClientPlugin • 0x6fac2:$b: ClientPlugin
00000011.00000002.383577417.0000000004539000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2080a5:$x1: NanoCore.ClientPluginHost • 0x23aac5:$x1: NanoCore.ClientPluginHost • 0x2080e2:$x2: IClientNetworkHost • 0x23ab02:$x2: IClientNetworkHost • 0x20bc15:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x23e635:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000011.00000002.383577417.0000000004539000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000011.00000002.383577417.000000000453 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x207e0d:$a: NanoCore • 0x207e1d:$a: NanoCore • 0x208051:$a: NanoCore • 0x208065:$a: NanoCore • 0x2080a5:$a: NanoCore • 0x23a82d:$a: NanoCore • 0x23a83d:$a: NanoCore • 0x23aa71:$a: NanoCore • 0x23aa85:$a: NanoCore • 0x23aac5:$a: NanoCore • 0x207e6c:$b: ClientPlugin • 0x20806e:$b: ClientPlugin • 0x2080ae:$b: ClientPlugin • 0x23a88c:$b: ClientPlugin • 0x23aa8e:$b: ClientPlugin • 0x23aace:$b: ClientPlugin • 0x154512:$c: ProjectData • 0x207f93:$c: ProjectData • 0x23a9b3:$c: ProjectData • 0x20899a:$d: DESCrypto • 0x23b3ba:$d: DESCrypto
Click to see the 33 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
28.2.dhcpmon.exe.2e09660.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
28.2.dhcpmon.exe.2e09660.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
22.2.m72OvSF7e5.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
22.2.m72OvSF7e5.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
22.2.m72OvSF7e5.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 75 entries				

Sigma Overview

System Summary:

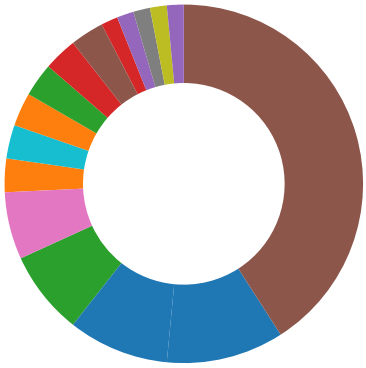
Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

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

Remote Access Functionality



Click to jump to signature section

AV Detection:

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

Compliance:

- Uses 32bit PE files
- Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

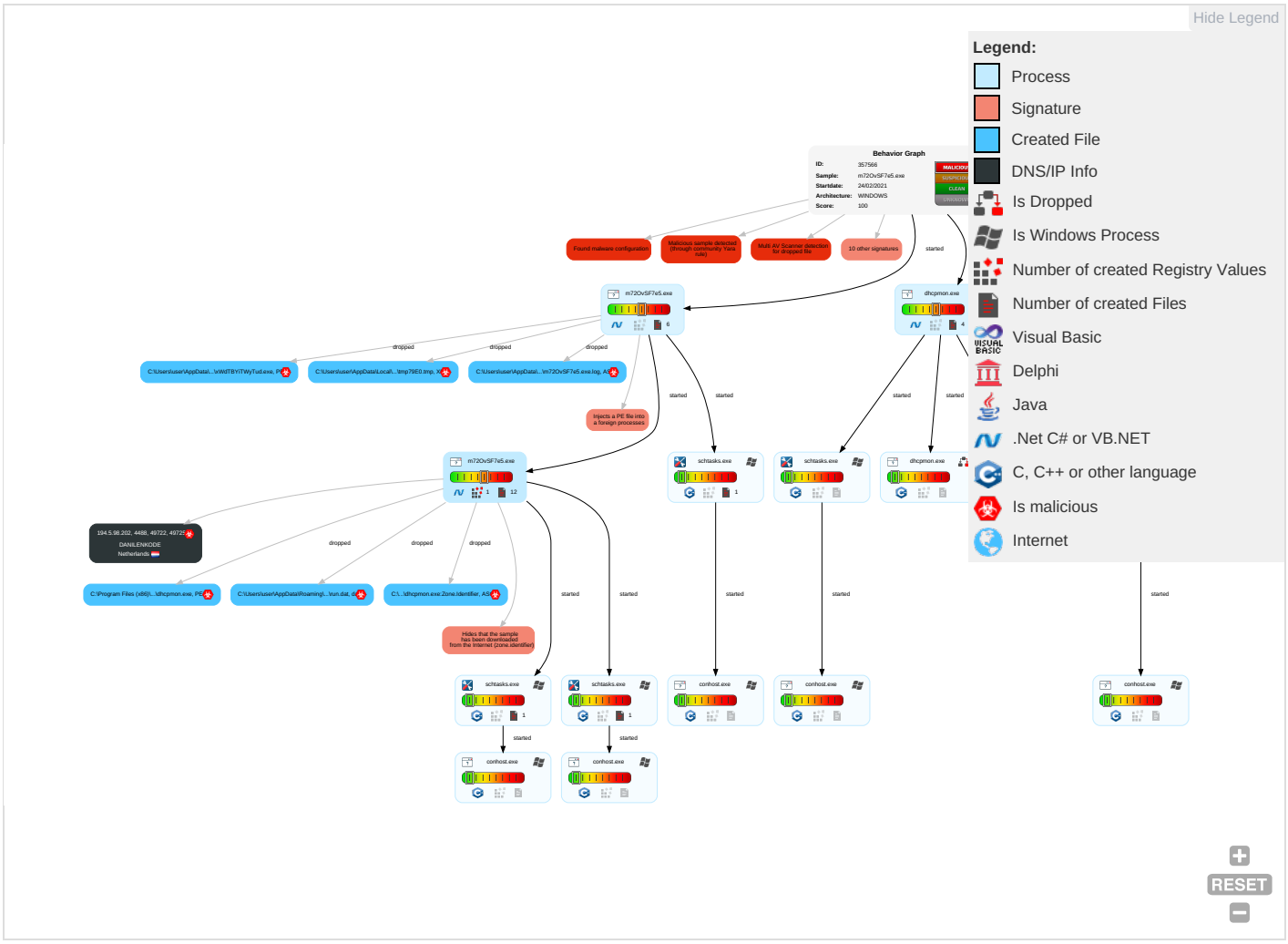
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 2	Input Capture 1 1	Security Software Discovery 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	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 1	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 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	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 2	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

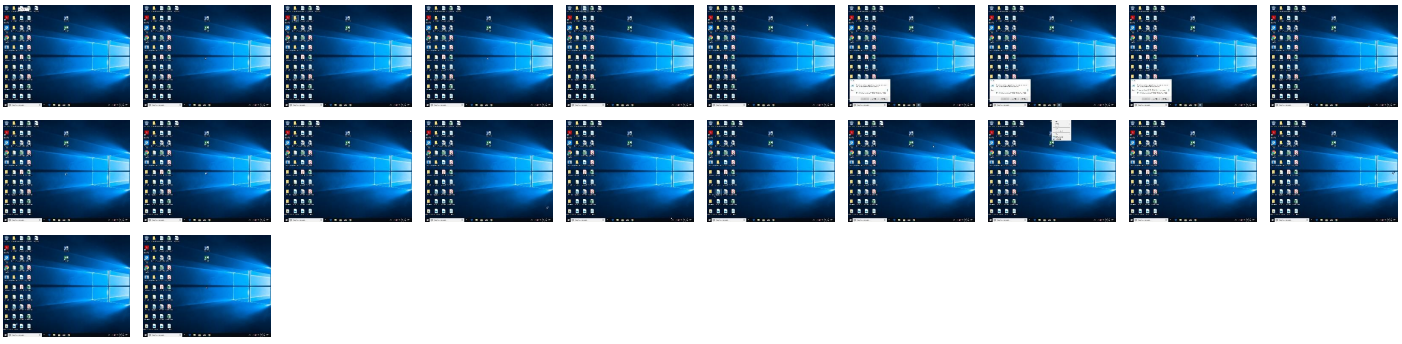
Behavior Graph



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

Source	Detection	Scanner	Label	Link
m72OvSF7e5.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
m72OvSF7e5.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\xWdTBYiTWyTud.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\xWdTBYiTWyTud.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.2.m72OvSF7e5.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
28.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.urwpp.dett	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnr-f6	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnskQ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicro	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.sandoll.co.krom	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnradM	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.tiro.comE	0%	Avira URL Cloud	safe	
http://www.sakkal.comw	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	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.founder.com.cn/cnht	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.founder.com.cn/cnn	0%	Avira URL Cloud	safe	
http://www.carterandcone.comaW	0%	Avira URL Cloud	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.tiro.comicw	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.carterandcone.comue	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html4	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.urwpp.de)	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.carterandcone.comicy	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	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn-u	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnicy	0%	Avira URL Cloud	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.carterandcone.comrose	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnw	0%	Avira URL Cloud	safe	
http://www.carterandcone.comose	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/J	0%	Avira URL Cloud	safe	
http://www.carterandcone.comdd	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-uC	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnk	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
194.5.98.202	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersH	m72OvSF7e5.exe, 00000000.00000003.253378838.0000000005F4B000.00000004.00000001.sdmp	false		high
http://www.urwpp.dett	m72OvSF7e5.exe, 00000000.00000003.253091287.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnr-f6	m72OvSF7e5.exe, 00000000.00000003.248450656.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersB	m72OvSF7e5.exe, 00000000.00000003.260543521.0000000005F4B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnskQ	m72OvSF7e5.exe, 00000000.00000003.248268109.0000000005F54000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnicro	m72OvSF7e5.exe, 00000000.00000003.248605286.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.krom	m72OvSF7e5.exe, 00000000.00000003.247254700.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnradM	m72OvSF7e5.exe, 00000000.00000003.248011341.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers0.	m72OvSF7e5.exe, 00000000.00000003.255198714.0000000005F4B000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	m72OvSF7e5.exe, 00000000.00000003.247308479.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000003.248662022.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000003.248728208.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comE	m72OvSF7e5.exe, 00000000.00000003.249291724.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.comw	m72OvSF7e5.exe, 00000000.00000003.250673385.0000000005F53000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comiona	m72OvSF7e5.exe, 00000000.00000002.305740597.0000000001777000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000003.245181004.0000000005F32000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnht	m72OvSF7e5.exe, 00000000.00000003.247627336.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnn	m72OvSF7e5.exe, 00000000.00000003.248268109.0000000005F54000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comaW	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	m72OvSF7e5.exe, 00000000.00000003.257585115.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

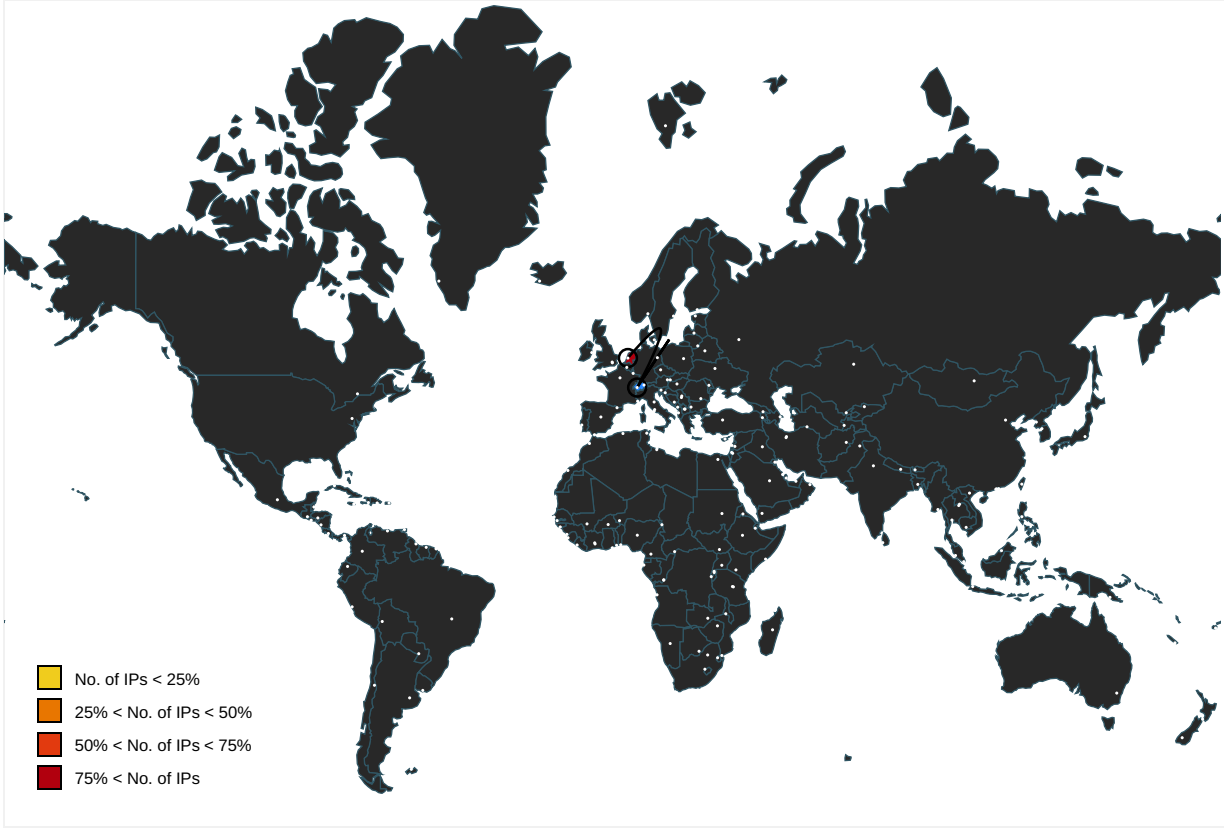
Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	m72OvSF7e5.exe, 00000000.00000003.245970853.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comicw	m72OvSF7e5.exe, 00000000.00000003.249291724.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersl	m72OvSF7e5.exe, 00000000.00000003.253911707.0000000005F4B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnl	m72OvSF7e5.exe, 00000000.00000003.248011341.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comue	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html4	m72OvSF7e5.exe, 00000000.00000003.251201016.0000000005F53000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de)	m72OvSF7e5.exe, 00000000.00000003.253091287.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ascendercorp.com/typedesigners.html	m72OvSF7e5.exe, 00000000.00000003.251201016.0000000005F53000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000003.250673385.0000000005F53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comicy	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	m72OvSF7e5.exe, 00000000.00000003.247154026.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000003.247254700.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	m72OvSF7e5.exe, 00000000.00000003.255571821.0000000005F57000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000003.248662022.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	m72OvSF7e5.exe, 00000000.00000002.305822663.0000000003091000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.381501971.0000000003A8D000.00000004.00000001.sdmp, dhcpmon.exe, 00000013.00000002.413950929.0000000002BCD000.00000004.00000001.sdmp	false		high
http://www.carterandcone.como.	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn-u	m72OvSF7e5.exe, 00000000.00000003.248450656.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000002.305740597.0000000001777000.00000004.00000040.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cnicy	m72OvSF7e5.exe, 00000000.00000003.248450656.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.come	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comc	m72OvSF7e5.exe, 00000000.00000003.249104893.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comrose	m72OvSF7e5.exe, 00000000.00000003.248662022.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	m72OvSF7e5.exe, 00000000.00000003.249104893.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnw	m72OvSF7e5.exe, 00000000.00000003.248450656.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comose	m72OvSF7e5.exe, 00000000.00000003.249291724.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/J	m72OvSF7e5.exe, 00000000.00000003.247848656.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comdd	m72OvSF7e5.exe, 00000000.00000003.249104893.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-uC	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comk	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnk	m72OvSF7e5.exe, 00000000.00000003.248450656.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	m72OvSF7e5.exe, 00000000.00000003.247308479.0000000005F4B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	m72OvSF7e5.exe, 00000000.00000003.254576087.0000000005F4B000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000000.00000003.254558630.0000000005F6E000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.html	m72OvSF7e5.exe, 00000000.00000003.255140115.0000000005F6E000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comEacl	m72OvSF7e5.exe, 00000000.00000003.249291724.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	m72OvSF7e5.exe, 00000000.00000002.326876582.0000000007142000.00000004.00000001.sdmp, m72OvSF7e5.exe, 00000011.00000002.389482810.0000000006270000.00000002.00000001.sdmp, dhcpmon.exe, 00000012.00000002.382162455.00000000054F0000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.420285861.00000000055F0000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comWfu	m72OvSF7e5.exe, 00000000.00000003.248802056.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comueu	m72OvSF7e5.exe, 00000000.00000003.249291724.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com%f	m72OvSF7e5.exe, 00000000.00000003.248981947.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/	m72OvSF7e5.exe, 00000000.00000003.253378838.0000000005F4B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn(	m72OvSF7e5.exe, 00000000.00000003.247627336.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.:	m72OvSF7e5.exe, 00000000.00000003.257160739.0000000005F4B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.202	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357566
Start date:	24.02.2021
Start time:	18:38:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	m72OvSF7e5.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:	39
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@27/12@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 71.2% • Quality standard deviation: 36.9%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • 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 NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/357566/sample/m72OvSF7e5.exe

Simulations

Behavior and APIs

Time	Type	Description
18:40:03	API Interceptor	697x Sleep call for process: m72OvSF7e5.exe modified
18:40:27	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\m72OvSF7e5.exe" s>$(Arg0)
18:40:27	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:40:31	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
18:40:36	API Interceptor	3x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.202	V33QokMrIv.exe	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	Eingang.Jpg.exe	Get hash	malicious	Browse	• 194.5.97.116
	V33QokMrIv.exe	Get hash	malicious	Browse	• 194.5.98.202
	3Fv4j323nj.exe	Get hash	malicious	Browse	• 194.5.98.182
	scan09e8902093922023ce.exe	Get hash	malicious	Browse	• 194.5.98.46
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 194.5.98.182

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 194.5.98.202
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	Orderoffer.exe	Get hash	malicious	Browse	• 194.5.98.66
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	• 194.5.97.248
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 194.5.97.244
	QuotationInvoices.exe	Get hash	malicious	Browse	• 194.5.97.248
	PAYMENT_.EXE	Get hash	malicious	Browse	• 194.5.98.211
	payment.exe	Get hash	malicious	Browse	• 194.5.98.66
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 194.5.98.21
	Slip copy .xls.exe	Get hash	malicious	Browse	• 194.5.97.116
	Scan0059.pdf.exe	Get hash	malicious	Browse	• 194.5.97.34
	DHL AWB # 6008824216.png.exe	Get hash	malicious	Browse	• 194.5.97.48
	Scan0019.exe	Get hash	malicious	Browse	• 194.5.97.34

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\xWdTBYiTWyTud.exe	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	766976
Entropy (8bit):	7.940274777998683
Encrypted:	false
SSDEEP:	12288:sEoF4lSePJI+f8Y+6l7MoPrYeAZDGfQ0lSzujpMEOoeYw3LLUEMthvoPTG16KL:GYPJnf876l7KTZDYizutM3oeLCsG16KL
MD5:	8C596990203F7D15651498FDBA84B5F3
SHA1:	BCABAE5C0B3CA8E9558AD3F57C3A10E8B5AE6F74
SHA-256:	A98A739B9AB7B06BF2833F6EF4AA97DB1B7C2441365C7104E878C8B29BF90F74
SHA-512:	1CBC6440FE45B66E5A72A41312B1195E25B64EDE5F97BFDE98CD9FDCABE30C9434FCEED40282D2453B7B25823AAEF7CB26F4D910E1EBA6FB95FB2A83D3968D93
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`.....0..... .....@.. ..... ..... ..@.....O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....Ho..p3.....4.....%.....&.(.....*...0..9.....~.....,".r...p.....(....o....s.....~.....+..*....0.....~.....+..*"".....*.0 ..!.....(....r!..p~....o.....t.....+..*....0..!.....(....r1..p~....o.....t.....+..*....0.....r5..p.+..*..0.....rA..p.+..*".(.....*^..}.....(.....(%....**...(.....*..0..;.....rQ..pr...p.(.....,..(.... ..+..s.....o .....(!.....*..0..I.....r...pr...p.(.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\m72OvSF7e5.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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\m72OvSF7e5.exe.log	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp2CE4.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.176206395814203
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBUtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3E
MD5:	0ED283E09C831888474411E9B6B1CA70
SHA1:	5D3E96B7D4E39DDE90DEE567170FA04D28F5BBE7
SHA-256:	1DAC39E417775EC539C9953DFB013CAEFC1B76C78D5C989E71F16F60192ECD8D
SHA-512:	6F3182A1BB764DBB319165124A640083BD0CE255F32E664B905528F52106D8018E73924EB032C0EE59EF01D37EA331123F38C13281471FD1DB29CB678BB8CDAE
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp2CE4.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp79E0.tmp	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.176206395814203
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBUtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3E
MD5:	0ED283E09C831888474411E9B6B1CA70
SHA1:	5D3E96B7D4E39DDE90DEE567170FA04D28F5BBE7
SHA-256:	1DAC39E417775EC539C9953DFB013CAEFC1B76C78D5C989E71F16F60192ECD8D
SHA-512:	6F3182A1BB764DBB319165124A640083BD0CE255F32E664B905528F52106D8018E73924EB032C0EE59EF01D37EA331123F38C13281471FD1DB29CB678BB8CDAE
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp84A.tmp	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	5.111047452277609
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Mxtn:cbk4oL600QydbQxIYODOLedq3fj
MD5:	3B021150D732CE9C1B83583CBBAB65B0
SHA1:	7AB50F74F9379D2CE4F71ABE69DB6318A81E3E59
SHA-256:	BFFB90288DD6A2FC0FAFEDB06DEFEDA15979230733F2FD9A77ABFD4B1AF44F8A
SHA-512:	ECB490FB065A9D7C53F8B8E3735900D61CDBCD5A5229AEDC6582EBC4ED600E4D6FE8A01156CE91A27E2C9FDEA692156162D3CD3F6709657177E9EF651C3E0EAE
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\Local\Temp\tmpE27.tmp	
Process:	C:\Users\user\Desktop\m72OvSF7e5.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

C:\Users\user\AppData\Local\Temp\tmpE27.tmp	
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\tmpF7E9.tmp	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.176206395814203
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBUtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3E
MD5:	0ED283E09C831888474411E9B6B1CA70
SHA1:	5D3E96B7D4E39DDE90DEE567170FA04D28F5BBE7
SHA-256:	1DAC39E417775EC539C9953DFB013CAEFC1B76C78D5C989E71F16F60192ECD8D
SHA-512:	6F3182A1BB764DBB319165124A640083BD0CE255F32E664B905528F52106D8018E73924EB032C0EE59EF01D37EA331123F38C13281471FD1DB29CB678BB8CDAE
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:wlm:wM
MD5:	A09BECF4F09438D33917C5B8E0D8665A
SHA1:	6E189F54EFF9747C8C4294B84390CEE3FAFB27D6
SHA-256:	0B2B27FDB63119E3504818C3A080F5499F69F9B67673C9E1B06365EA5A25E73E
SHA-512:	1C913FD38916398CF4FD0652169E91927ABDDBCB9B2D31A9B59D0D7D22A63C9F5C204139602D4F79D3A2715242521FA2EAB9B132DA51D30485DEA861E55C08D
Malicious:	**true**
Preview:	....6..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.345118467927183
Encrypted:	false
SSDEEP:	3:oN0naRRIuA:oNcSRIuA
MD5:	CAA1DF014F8918E60F42746A155DABF8
SHA1:	AC61D00144FE9F813FF1E5F91E2E5C738319FE73
SHA-256:	C7A609BA17D183FFAABDAA9A6F28270D508CDE2A09ABD99EE1CD3E60382A3240
SHA-512:	024D7F902A8D2B49B481BA11C428BD3EF9065A11397585626EA2D1D0F4C4DED093B01D1E22DCDCEFC155769BA57A78FD461E6A98E8E4FC15CF05349BFDA0B2BF
Malicious:	false
Preview:	C:\Users\user\Desktop\m72OvSF7e5.exe

C:\Users\user\AppData\Roaming\xWdTBYiTWyTud.exe	
Process:	C:\Users\user\Desktop\m72OvSF7e5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	766976
Entropy (8bit):	7.940274777998683

C:\Users\user\AppData\Roaming\xWdTBYiTWyTud.exe	
Encrypted:	false
SSDEEP:	12288:sEoF4lSePJI+f8Y+6I7MoPrYeAZDGfQ0lSzujpMEOoeYw3LLUEMthvoPTG16KL:GYPJnf876I7KTZDYizutM3oeLCsG16KL
MD5:	8C596990203F7D15651498FDBA84B5F3
SHA1:	BCABAE5C0B3CA8E9558AD3F57C3A10E8B5AE6F74
SHA-256:	A98A739B9AB7B06BF2833F6EF4AA97DB1B7C2441365C7104E878C8B29BF90F74
SHA-512:	1CBC6440FE45B66E5A72A41312B1195E25B64EDE5F97BFDE98CD9FDCABE30C9434FCEED40282D2453B7B25823AAEF7CB26F4D910E1EBA6FB95FB2A83D3968D93
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`.....0..... ..... @.. ..... ..... ..@.....O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....Ho..p3.....4.....%.....&.(.....*...0..9.....~.....,".r...p.....(....o....s.....~.....+..*....0.....~.....+..*"".....*.0 ..!.....(....r!..p~....o.....t.....+..*....0..!.....(....r1..p~....o.....t.....+..*....0.....r5..p.+..*..0.....rA..p.+..*".(.....*^..}.....(.....(%....**...(.....*..0..;.....rQ..pr...p.(.....,..(.... ..+..s.....o .....(!....*..0..I.....r...pr...p.(.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.940274777998683
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	m72OvSF7e5.exe
File size:	766976
MD5:	8c596990203f7d15651498fdba84b5f3
SHA1:	bcabae5c0b3ca8e9558ad3f57c3a10e8b5ae6f74
SHA256:	a98a739b9ab7b06bf2833f6ef4aa97db1b7c2441365c7104e878c8b29bf90f74
SHA512:	1cbc6440fe45b66e5a72a41312b1195e25b64ede5f97bfde98cd9fdcabe30c9434fceed40282d2453b7b25823aaef7cb26f4d910e1eba6fb95fb2a83d3968d93
SSDEEP:	12288:sEoF4lSePJI+f8Y+6I7MoPrYeAZDGfQ0lSzujpMEOoeYw3LLUEMthvoPTG16KL:GYPJnf876I7KTZDYizutM3oeLCsG16KL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`.....0..... ..... @.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bc80a
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:	0x6035D91A [Wed Feb 24 04:42:02 2021 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbc7b8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text

Name	Virtual Address	Virtual Size	Is in Section
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	0xba810	0xbaa00	False	0.932769591427	data	7.94577186354	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x5b4	0x600	False	0.432942708333	data	4.21052745269	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbe090	0x324	data		
RT_MANIFEST	0xbe3c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	4.0.0.0
InternalName	TGk5J.exe
FileVersion	4.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ITP_RMSS
ProductVersion	4.0.0.0
FileDescription	ITP_RMSS
OriginalFilename	TGk5J.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 18:40:31.957748890 CET	49722	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:32.234703064 CET	4488	49722	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:32.763605118 CET	49722	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:33.066901922 CET	4488	49722	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:33.654454947 CET	49722	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:34.105788946 CET	4488	49722	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:38.740267992 CET	49725	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:39.021805048 CET	4488	49725	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:39.686141014 CET	49725	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:39.966897011 CET	4488	49725	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:40.483031034 CET	49725	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:40.766974926 CET	4488	49725	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:46.861275911 CET	49728	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:47.131726027 CET	4488	49728	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:47.655553102 CET	49728	4488	192.168.2.7	194.5.98.202

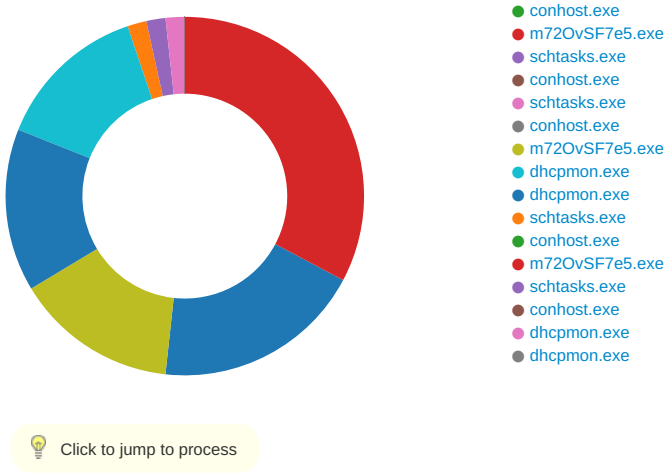
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 18:40:47.930370092 CET	4488	49728	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:48.561847925 CET	49728	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:48.831370115 CET	4488	49728	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:54.363543987 CET	49729	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:54.641540051 CET	4488	49729	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:55.187378883 CET	49729	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:55.465792894 CET	4488	49729	194.5.98.202	192.168.2.7
Feb 24, 2021 18:40:55.984328032 CET	49729	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:40:56.256597042 CET	4488	49729	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:00.267158985 CET	49730	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:00.547666073 CET	4488	49730	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:01.187942028 CET	49730	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:01.488466978 CET	4488	49730	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:02.136231899 CET	49730	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:02.431296110 CET	4488	49730	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:06.447145939 CET	49736	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:06.725570917 CET	4488	49736	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:07.266489029 CET	49736	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:07.545663118 CET	4488	49736	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:08.157237053 CET	49736	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:08.426438093 CET	4488	49736	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:12.549977064 CET	49737	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:12.818486929 CET	4488	49737	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:13.329555035 CET	49737	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:13.609318018 CET	4488	49737	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:14.127358913 CET	49737	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:14.393717051 CET	4488	49737	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:18.433444977 CET	49738	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:18.716609955 CET	4488	49738	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:19.221802950 CET	49738	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:19.501626968 CET	4488	49738	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:20.006016016 CET	49738	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:20.287722111 CET	4488	49738	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:24.374414921 CET	49739	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:24.666488886 CET	4488	49739	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:25.174283981 CET	49739	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:25.456455946 CET	4488	49739	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:25.971285105 CET	49739	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:26.269743919 CET	4488	49739	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:30.285620928 CET	49740	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:30.551568985 CET	4488	49740	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:31.065418959 CET	49740	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:31.341623068 CET	4488	49740	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:31.846676111 CET	49740	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:32.120675087 CET	4488	49740	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:36.130944014 CET	49742	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:36.407356977 CET	4488	49742	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:36.909609079 CET	49742	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:37.216361046 CET	4488	49742	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:37.722147942 CET	49742	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:38.044959068 CET	4488	49742	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:42.052165985 CET	49743	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:42.336393118 CET	4488	49743	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:42.847588062 CET	49743	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:43.128284931 CET	4488	49743	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:43.628968000 CET	49743	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:43.920660019 CET	4488	49743	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:47.927405119 CET	49744	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:50.942068100 CET	49744	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:51.221467018 CET	4488	49744	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:51.723417044 CET	49744	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:51.996634960 CET	4488	49744	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:56.006624937 CET	49750	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:56.276757002 CET	4488	49750	194.5.98.202	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 18:41:56.786268950 CET	49750	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:57.055735111 CET	4488	49750	194.5.98.202	192.168.2.7
Feb 24, 2021 18:41:57.567692041 CET	49750	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:41:57.841870070 CET	4488	49750	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:01.884973049 CET	49754	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:02.181546926 CET	4488	49754	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:02.724307060 CET	49754	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:03.006623030 CET	4488	49754	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:03.521239042 CET	49754	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:03.801537991 CET	4488	49754	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:07.842608929 CET	49755	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:08.130831003 CET	4488	49755	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:08.740433931 CET	49755	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:09.056885004 CET	4488	49755	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:09.742245913 CET	49755	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:10.026472092 CET	4488	49755	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:14.089448929 CET	49756	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:14.360654116 CET	4488	49756	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:14.912879944 CET	49756	4488	192.168.2.7	194.5.98.202
Feb 24, 2021 18:42:15.185463905 CET	4488	49756	194.5.98.202	192.168.2.7
Feb 24, 2021 18:42:15.725471973 CET	49756	4488	192.168.2.7	194.5.98.202

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: m72OvSF7e5.exe PID: 6316 Parent PID: 5740

General

Start time:	18:39:53
Start date:	24/02/2021

Path:	C:\Users\user\Desktop\m72OvSF7e5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\m72OvSF7e5.exe'
Imagebase:	0xc70000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.309611902.0000000004099000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.309611902.0000000004099000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.309611902.0000000004099000.00000004.00000001.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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Roaming\xWdTBYiTWyTud.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C211E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp79E0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\m72OvSF7e5.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp79E0.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xWdTBYiTWyTud.exe	unknown	766976	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 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 1a d9 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 aa 0b 00 00 08 00 00 00 00 00 00 0a c8 0b 00 00 20 00 00 00 e0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 20 0c 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.....5`..... ....0..... ....@.. ....@.....	success or wait	1	6C211B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp79E0.tmp	unknown	1662	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6C211B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\m72OvSF7e5.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile
C:\Users\user\Desktop\m72OvSF7e5.exe	unknown	766976	success or wait	1	6C211B4F	ReadFile

Analysis Process: schtasks.exe PID: 7104 Parent PID: 6316

General

Start time:	18:40:19
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWdTBYiTWyTud' /XML 'C:\Users\user\AppData\Local\Temp\tmp79E0.tmp'
Imagebase:	0x8f0000
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\tmp79E0.tmp	unknown	2	success or wait	1	8FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp79E0.tmp	unknown	1663	success or wait	1	8FABD9	ReadFile

Analysis Process: conhost.exe PID: 7144 Parent PID: 7104

General

Start time:	18:40:20
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: m72OvSF7e5.exe PID: 5808 Parent PID: 6316

General

Start time:	18:40:20
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\m72OvSF7e5.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x900000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D3CCF06	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	6D3CCF06	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	6C21BEFF	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	6C211E60	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	6C21BEFF	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	6C21DD66	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	6C21DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp84A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	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	6C211E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE27.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C21BEFF	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	6C21BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp84A.tmp	success or wait	1	6C216A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE27.tmp	success or wait	1	6C216A95	DeleteFileW
C:\Users\user\Desktop\m72OvSF7e5.exe:Zone.Identifier	success or wait	1	6C192935	unknown

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	0d 88 00 b4 36 d9 d8 48	....6..H	success or wait	1	6C211B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1a d9 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 aa 0b 00 00 08 00 00 00 00 00 00 0a c8 0b 00 00 20 00 00 00 e0 0b 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 20 0c 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.....5`.......... ....0.................. ....@.. ....@................	success or wait	3	6C21DD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C21DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp84A.tmp	unknown	1304	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	6C211B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	41	43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 44 65 73 6b 74 6f 70 5c 6d 37 32 4f 76 53 46 37 65 35 2e 65 78 65	C:\Users\user\Desktop\m7 2OvSF7e5.exe	success or wait	1	6C211B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE27.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	6C211B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D38D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D38D72F	unknown
C:\Users\user\Desktop\m72OvSF7e5.exe	unknown	4096	success or wait	1	6D38D72F	unknown
C:\Users\user\Desktop\m72OvSF7e5.exe	unknown	512	success or wait	1	6D38D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C21646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 5404 Parent PID: 5808

General

Start time:	18:40:25
Start date:	24/02/2021
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\tmp84A.tmp'
Imagebase:	0x8f0000
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\tmp84A.tmp	unknown	2	success or wait	1	8FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp84A.tmp	unknown	1305	success or wait	1	8FABD9	ReadFile

Analysis Process: conhost.exe PID: 6112 Parent PID: 5404

General

Start time:	18:40:25
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6412 Parent PID: 5808

General

Start time:	18:40:26
Start date:	24/02/2021
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\tmpE27.tmp'
Imagebase:	0x8f0000
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\tmpE27.tmp	unknown	2	success or wait	1	8FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE27.tmp	unknown	1311	success or wait	1	8FABD9	ReadFile

Analysis Process: conhost.exe PID: 6548 Parent PID: 6412

General

Start time:	18:40:27
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: m72OvSF7e5.exe PID: 6620 Parent PID: 1104

General

Start time:	18:40:28
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\m72OvSF7e5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\m72OvSF7e5.exe 0
Imagebase:	0xdc0000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
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: 00000011.00000002.383577417.0000000004539000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.383577417.0000000004539000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.383577417.0000000004539000.00000004.00000001.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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpF7E9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF7E9.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF7E9.tmp	unknown	1662	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">..<RegistrationInfo>..<Date>2014-10-25T14:27:44.8929027</Date>..<Author>computer\user</Author>..</Registrati	success or wait	1	6C211B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 4608 Parent PID: 1104

General

Start time:	18:40:31
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x1c0000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
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: 00000012.00000002.372726436.0000000003539000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.372726436.0000000003539000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.372726436.0000000003539000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, 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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 404 Parent PID: 3292

General

Start time:	18:40:35
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x270000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
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: 00000013.00000002.416135404.0000000003B47000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.416135404.0000000003B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.416135404.0000000003B47000.00000004.00000001.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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp2CE4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2CE4.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2CE4.tmp	unknown	1662	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6C211B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: schtasks.exe PID: 3276 Parent PID: 6620

General

Start time:	18:40:52
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWdTBYiTWyTud' /XML 'C:\Users\user\AppData\Local\Temp\tmpF7E9.tmp'
Imagebase:	0x8f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 4696 Parent PID: 3276

General

Start time:	18:40:52
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: m72OvSF7e5.exe PID: 6096 Parent PID: 6620

General

Start time:	18:40:53
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\m72OvSF7e5.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaa0000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
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: 00000016.00000002.392744009.0000000002E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.392744009.0000000002E71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.390672514.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.390672514.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.390672514.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.392926615.0000000003E79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.392926615.0000000003E79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: schtasks.exe PID: 2144 Parent PID: 404

General

Start time:	18:41:06
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWdTBYiTWyTud' /XML 'C:\Users\user\AppData\Local\Temp\tmp2CE4.tmp'
Imagebase:	0x8f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5408 Parent PID: 2144

General

Start time:	18:41:08
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 6984 Parent PID: 404

General

Start time:	18:41:09
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x390000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5724 Parent PID: 404

General

Start time:	18:41:09
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa30000
File size:	766976 bytes
MD5 hash:	8C596990203F7D15651498FDBA84B5F3
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: 0000001C.00000002.427245821.0000000003DA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.427245821.0000000003DA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.427149067.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.427149067.0000000002DA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000002.425873498.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.425873498.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.425873498.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis