ID: 552771
Sample Name:
TT#U007e)9383763563783039847949N.cmd.exe
Cookbook: default.jbs
Time: 18:02:36
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

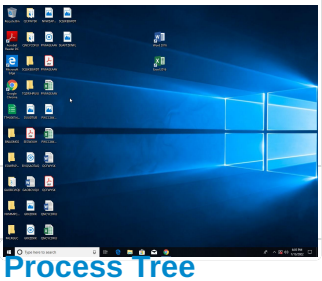
Windows Analysis Report TT#U007e)9383763563783039…

Overview

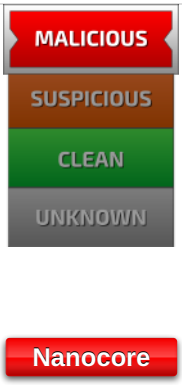
General Information

Sample Name:	TT#U007e)9383763563783039847949N.cmd.exe
Analysis ID:	552771
MD5:	398e8790480f654.
SHA1:	5cf487848131368.
SHA256:	c839234f96d6ce5..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



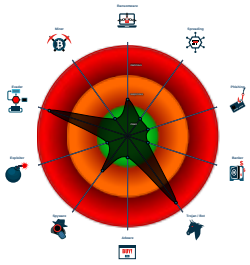
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…

Classification



Process Tree

- **System is w10x64**
- TT#U007e)9383763563783039847949N.cmd.exe (PID: 6280 cmdline: "C:\Users\user\Desktop\TT#U007e)9383763563783039847949N.cmd.exe" MD5: 398E8790480F654B4D677847BA454560)
  - powershell.exe (PID: 6768 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\wUDpvSE.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6788 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\wUDpvSE" /XML "C:\Users\user\AppData\Local\Temp\tmp1EE6.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6956 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - schtasks.exe (PID: 2672 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp3840.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 3724 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp42FF.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 476 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6636 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 3748 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "423b1032-a4e4-4490-8998-68a509ca",
  "Group": "",
  "Domain1": "55098hustlenow.hopto.org",
  "Domain2": "185.140.53.130",
  "Port": 55098,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "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
0000000A.00000002.517211527.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000002.517211527.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000002.517211527.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000A.00000002.523432863.00000000059D0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
0000000A.00000002.523432863.00000000059D0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.RegSvcs.exe.41b4c55.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x24178:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x241a5:$x2: IClientNetworkHost
10.2.RegSvcs.exe.41b4c55.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x24178:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x25253:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x24192:$s5: IClientLoggingHost
10.2.RegSvcs.exe.41b4c55.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.TT#U007e)9383763563783039847949N.cmd .exe.3b2b8b0.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.TT#U007e)9383763563783039847949N.cmd .exe.3b2b8b0.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
Click to see the 59 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

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)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

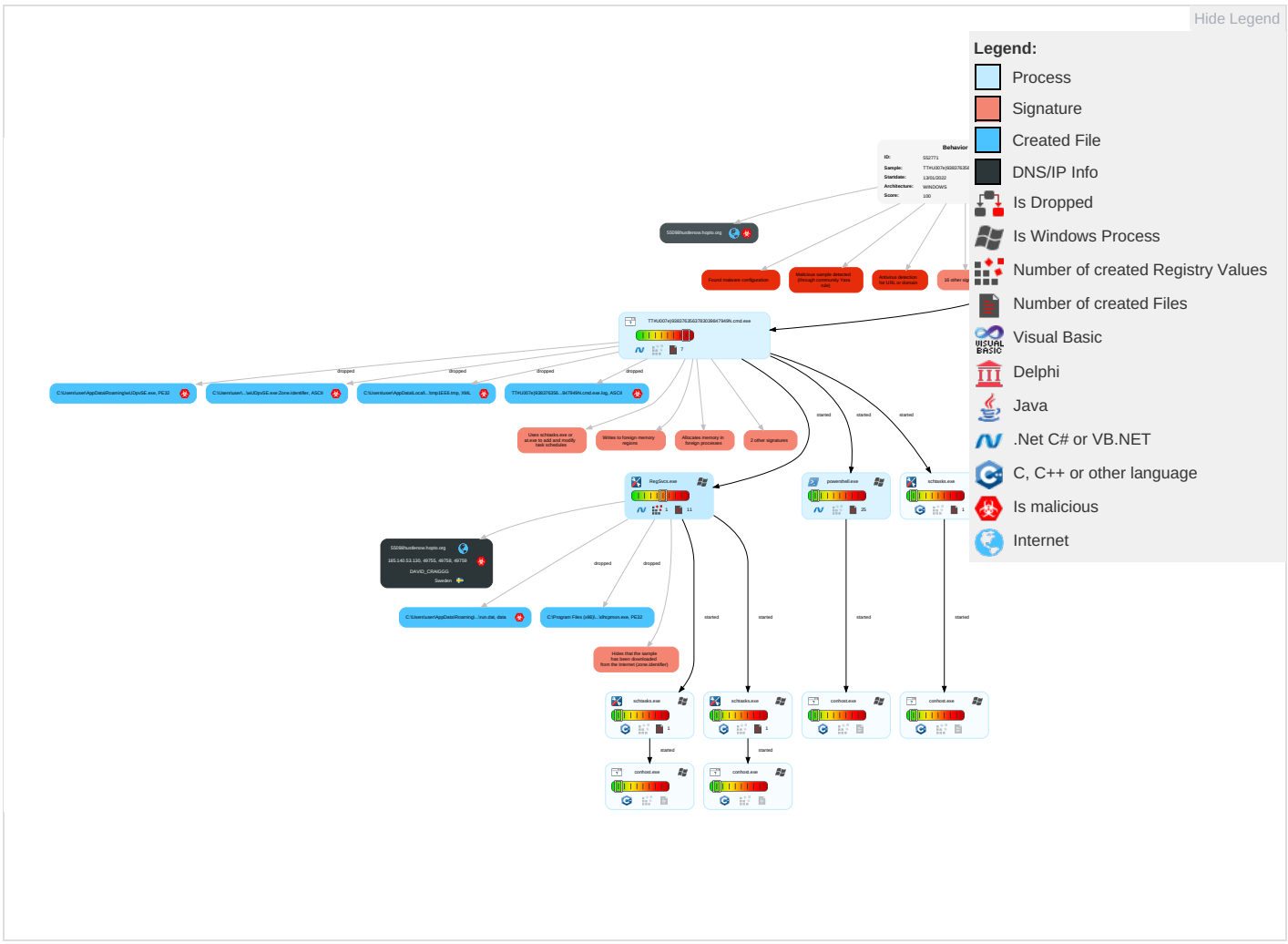
Detected Nanocore Rat

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 3 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 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 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System 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

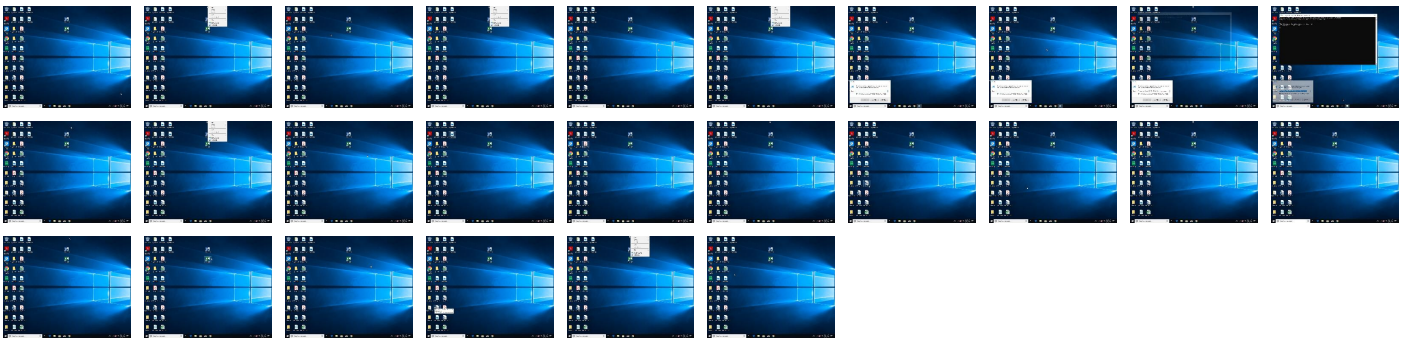
Behavior Graph



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
TT#U007e)9383763563783039847949N.cmd.exe	31%	Virustotal		Browse
TT#U007e)9383763563783039847949N.cmd.exe	32%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
TT#U007e)9383763563783039847949N.cmd.exe	100%	Avira	HEUR/AGEN.1211287	
TT#U007e)9383763563783039847949N.cmd.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\wUDpvSE.exe	100%	Avira	HEUR/AGEN.1211287	
C:\Users\user\AppData\Roaming\wUDpvSE.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\wUDpvSE.exe	32%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.TT#U007e)9383763563783039847949N.cmd.exe.640000.0.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
10.2.RegSvcs.exe.5a70000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
0.0.TT#U007e)9383763563783039847949N.cmd.exe.640000.0.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
10.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
55098hustlenow.hopto.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/staff/dennis.htmsKi	0%	Avira URL Cloud	safe	
http://www.urwpp.de1Yq	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiviV	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.com#	0%	Avira URL Cloud	safe	
http://www.carterandcone.comoup	0%	Avira URL Cloud	safe	
http://www.urwpp.deld	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnark	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
55098hustlenow.hopto.org	100%	Avira URL Cloud	malware	
http://www.sakkal.comAY	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comintPM5	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	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.urwpp.deoimY	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comngH	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cncom	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn#	0%	Avira URL Cloud	safe	
http://www.carterandcone.comEac	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html-KS	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.carterandcone.como.Z	0%	Avira URL Cloud	safe	
http://www.carterandcone.comtig	0%	URL Reputation	safe	
http://www.urwpp.depY0	0%	Avira URL Cloud	safe	
185.140.53.130	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://www.carterandcone.comf	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.fontbureau.comH	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/D	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krim2NV	0%	Avira URL Cloud	safe	
http://www.tiro.com6Yv	0%	Avira URL Cloud	safe	
http://www.carterandcone.comlt	0%	URL Reputation	safe	
http://www.sajatypeworks.comGD	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.compt	0%	Avira URL Cloud	safe	
http://www.monotype.FM	0%	Avira URL Cloud	safe	
http://www.carterandcone.comi	0%	URL Reputation	safe	
http://www.carterandcone.comh	0%	URL Reputation	safe	
http://www.carterandcone.comTC8Zk	0%	Avira URL Cloud	safe	
http://www.fontbureau.comc	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.urwpp.deHY	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cnof	0%	Avira URL Cloud	safe	
http://www.carterandcone.comark	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn#	0%	URL Reputation	safe	
http://www.fontbureau.comiona;	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.4_	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
55098hustlenow.hopto.org	185.140.53.130	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
55098hustlenow.hopto.org	true	• Avira URL Cloud: malware	unknown
185.140.53.130	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.130	55098hustlenow.hopto.org	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552771
Start date:	13.01.2022
Start time:	18:02:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TT#U007e)9383763563783039847949N.cmd.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:	38
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@21/18@12/1
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 10.1%) • Quality average: 36.7% • Quality standard deviation: 40%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:03:45	API Interceptor	2x Sleep call for process: TT#U007e)9383763563783039847949N.cmd.exe modified
18:03:50	API Interceptor	32x Sleep call for process: powershell.exe modified
18:03:57	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:04:00	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" s>$(Arg0)
18:04:01	API Interceptor	811x Sleep call for process: RegSvcs.exe modified
18:04:02	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(.... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TT#U007e)9383763563783039847949N.cmd.exe.log	
Process:	C:\Users\user\Desktop\TT#U007e)9383763563783039847949N.cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
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\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22304
Entropy (8bit):	5.602293803799045
Encrypted:	false
SSDEEP:	384:7tCDvq0SjiDhIZPlF+X0SBKncjultIC77Y9ghSJ3x6T1MavZlbAV70W0CS5ZBDIn:E1l5lQ04KcCltdfhcAC+fw8V8
MD5:	FA78CE6AE356D064695AF2BDD7341D32
SHA1:	0DDB53FEE435A0223E65E93D76CCEEC6A080B47D
SHA-256:	14AC2905BBBE4829DB4243E4F308740D102C37FB414CFD0505CE50244C893B64
SHA-512:	E762291E1F8FB2913028B6A2C2D57F25C098699701BC1FE4B24354FC48CDB0555E03699B08F9C99C71352F3CAE58FF9531FD9D0369F73EB6DCF00F29B41FC2CF
Malicious:	false
Preview:	@...e.....h.j.....U...H.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jj1by3vo.fw0.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_n3o5mldn.ubu.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp1EE6.tmp	
Process:	C:\Users\user\Desktop\TT#U007e)9383763563783039847949N.cmd.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1610
Entropy (8bit):	5.129004283554135
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtDVxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTnv
MD5:	A24B8E375AAA02A354B2941D3A96C606
SHA1:	8848F86B51434884FEBF51349E6C24A6265770C0
SHA-256:	446A5BC1AFF0C829A4F1DAD5B0855A172AB5164021B8FB67EE764A95D595CBF0
SHA-512:	34DD1225156DC0604532C84C1009BC462CFBC6B33D9AC61F71946502F4C2DCC77E80DA1C2947C13F620328C9E3C7424378EC2AB91037D3EA92BC7A78F66277A
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>. <StartWhenAvailable>true</StartWhenAvai

C:\Users\user\AppData\Local\Temp\tmp3840.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135668813522653
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mXxtn:cbk4oL600QydbQxIYODOLedq3ZXj
MD5:	8CAD1B41587CED0F1E74396794F31D58
SHA1:	11054BF74FCF5E8E412768035E4DAE43AA7B710F
SHA-256:	3086D914F6B23268F8A12CB1A05516CD5465C2577E1D1E449F1B45C8E5E8F83C
SHA-512:	99C2EF89029DE51A866DF932841684B7FC912DF21E10E2DD0D09E400203BBDC6CBA6319A31780B7BF8B286D2CEA8EA3FC7D084348BF2F002AB4F5A34218CCBF
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\tmp42FF.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Py8n:d
MD5:	612A3AAA3EB1E3046475CE7469453925
SHA1:	FB1074A68885D040D99F16FE7253FEA92EA01897
SHA-256:	E5D20EEFDF29305CFF4161CDE69900F2141E017A5E1B5B01DB8F342E513E16D9
SHA-512:	A793B1A88A446ADA623B5878B0F12B2BBA83C3C29976873313D9BCC1D9B5D8530647E97C60BB6825B759B36CA3E2497FFD7C8C2B381A6A4E17E91741181E8DB
Malicious:	**true**
Preview:	.j.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.830795005765378
Encrypted:	false
SSDEEP:	3:oMty8WddSWA1KMNn:oMLW6WA1j
MD5:	08E799E8E9B4FDA648F2500A40A11933
SHA1:	AC76B5E20DED247803448A2F586731ED7D84B9F3
SHA-256:	D46E34924067EB071D1F031C0BC015F4B711EDCE64D8AE00F24F29E73ECB71DB
SHA-512:	5C5701A86156D573BE274E73615FD6236AC89630714863A4CB2639EEC8EC1BE746839EBF8A9AEBA0A9BE326AF6FA02D8F9BD7A93D3FFB139BADE945572DF5FE9
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

C:\Users\user\AppData\Roaming\wUDpvSE.exe	
Process:	C:\Users\user\Desktop\TT#U007e)9383763563783039847949N.cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	636416
Entropy (8bit):	7.184563052963555
Encrypted:	false
SSDEEP:	12288:s0DK777777777777SfDTaWZq81e9infTaO5MgzV9MmvP:dK777777777777SfPaWZReMnfTPPzVx
MD5:	398E8790480F654B4D677847BA454560
SHA1:	5CF48784813136868BDF1D995500056EAEB702A2
SHA-256:	C839234F96D6CE5D83F511FF6AA0D0AFC7A680BC478C81416592C981BB066058
SHA-512:	BDFFC299BEA5E8AD084526B6430E934403C4A5C59710CE6222ED5A7EA211FC07BAFD507415166658538DCBDE2DC8AAB90696D2E64E3736CB071BBC3E669DE1F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...45.a.....2.....P... ...`....@.. ..... ..@.....P..W....`..... ....H.....text....0... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....@..B.....P.....H.....P"..H.....-...$^..,.....z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.....f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*.....n..}.....{.....,.{....oc...*..{....*.s..

C:\Users\user\AppData\Roaming\wUDpvSE.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\TT#U007e)9383763563783039847949N.cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220113\PowerShell_transcript.377142.s88OTTbR.20220113180347.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5817
Entropy (8bit):	5.382970840664857
Encrypted:	false
SSDEEP:	96:BZZ6KN2qDo1Z9ZW6KN2qDo1ZxkusjZW6KN2qDo1ZAp88KZ1:p
MD5:	22D5AAB9A5CE9A995C2975326DC44122
SHA1:	1FA995ACF40D3C05767A4BF3BCF8C7B2D5B0FD67
SHA-256:	16A3BDE7DEA8D671FA6AE99C54C5E584324682C862ADFC02CDCDF6C6FEAA87EB
SHA-512:	F118EBBAA330E9416C67636E7BBBA3D3C55B3B2E1671CCDE308330E415EB185EE7EE1A47241BCDE863EA1D914C7733C3BC8BDDBC0AD5555435E62734E6A10F2A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220113180350..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 377142 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\wUDpvSE.exe..Process ID: 6768..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220113180350..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\wUDpvSE.exe..**********..Windows PowerShell transcript start..Start time: 20220113180735..Username: computer\user..RunAs User: DESKTO

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.184563052963555
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:	TT#U007e)9383763563783039847949N.cmd.exe
File size:	636416
MD5:	398e8790480f654b4d677847ba454560
SHA1:	5cf48784813136868bdf1d995500056eaeb702a2
SHA256:	c839234f96d6ce5d83f511ff6aa0d0afc7a680bc478c81416592c981bb066058
SHA512:	bdffc299bea5e8ad084526b6430e934403c4a5c59710ce6222ed5a7ea211fc07bafd507415166658538dcbde2dc8aab90696d2e64e3736cb071bbc3e669deb1f
SSDEEP:	12288:s0DK777777777777SfDTaWZq81e9infTaO5MgzV9MmvP:dK777777777777SfPaWZReMnfTPPzVx

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...45.a.....2.....P... ...`....@.. .....@.....

File Icon

Icon Hash:	64cce4f4f4e4dcd4

Static PE Info

General

Entrypoint:	0x4750f2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E03534 [Thu Jan 13 14:20:36 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x730f8	0x73200	False	0.891795602606	data	7.78329348907	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x27fc8	0x28000	False	0.0971069335938	data	4.27505940425	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-18:04:03.012940	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60338	8.8.8.8	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-18:04:08.378279	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59762	8.8.8.8	192.168.2.7
01/13/22-18:04:13.815191	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54329	8.8.8.8	192.168.2.7
01/13/22-18:05:06.309288	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60983	8.8.8.8	192.168.2.7
01/13/22-18:05:11.492794	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49247	8.8.8.8	192.168.2.7
01/13/22-18:05:16.661585	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52286	8.8.8.8	192.168.2.7
01/13/22-18:05:37.804947	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63744	8.8.8.8	192.168.2.7
01/13/22-18:05:42.928983	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61457	8.8.8.8	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 18:04:02.991837025 CET	192.168.2.7	8.8.8.8	0xb5df	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:08.357667923 CET	192.168.2.7	8.8.8.8	0x4563	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:13.791904926 CET	192.168.2.7	8.8.8.8	0x8a19	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:34.693816900 CET	192.168.2.7	8.8.8.8	0x81c6	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:40.096425056 CET	192.168.2.7	8.8.8.8	0x3395	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:45.271754980 CET	192.168.2.7	8.8.8.8	0x925e	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:06.290409088 CET	192.168.2.7	8.8.8.8	0x87ab	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:11.471663952 CET	192.168.2.7	8.8.8.8	0xea24	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:16.642559052 CET	192.168.2.7	8.8.8.8	0x90a2	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:37.786194086 CET	192.168.2.7	8.8.8.8	0xb6be	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:42.908484936 CET	192.168.2.7	8.8.8.8	0xbb12	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:48.033751011 CET	192.168.2.7	8.8.8.8	0xb2f8	Standard query (0)	55098hustl enow.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 18:04:03.012939930 CET	8.8.8.8	192.168.2.7	0xb5df	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:08.378278971 CET	8.8.8.8	192.168.2.7	0x4563	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:13.815191031 CET	8.8.8.8	192.168.2.7	0x8a19	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:34.714128971 CET	8.8.8.8	192.168.2.7	0x81c6	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:04:40.115456104 CET	8.8.8.8	192.168.2.7	0x3395	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 18:04:45.291075945 CET	8.8.8.8	192.168.2.7	0x925e	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:06.309288025 CET	8.8.8.8	192.168.2.7	0x87ab	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:11.492794037 CET	8.8.8.8	192.168.2.7	0xea24	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:16.661585093 CET	8.8.8.8	192.168.2.7	0x90a2	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:37.804946899 CET	8.8.8.8	192.168.2.7	0xb6be	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:42.928982973 CET	8.8.8.8	192.168.2.7	0xbb12	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)
Jan 13, 2022 18:05:48.053014040 CET	8.8.8.8	192.168.2.7	0xb2f8	No error (0)	55098hustl enow.hopto.org		185.140.53.130	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: TT#U007e)938376356378303984794 9N.cmd.exe PID: 6280 Parent PID: 2412

General

Start time:	18:03:34
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\TT#U007e)938376356378303984794 9N.cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TT#U007e)938376356378303984794 9N.cmd.exe"
Imagebase:	0x640000
File size:	636416 bytes
MD5 hash:	398E8790480F654B4D677847BA454560
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.290665928.0000000002B05000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.290448066.0000000002A11000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.291731877.0000000003A19000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.291731877.0000000003A19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.291731877.0000000003A19000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6768 Parent PID: 6280

General

Start time:	18:03:46
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\wUDpvSE.exe
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6780 Parent PID: 6768

General

Start time:	18:03:46
Start date:	13/01/2022
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: 6788 Parent PID: 6280

General

Start time:	18:03:47
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\wUDpvSE" /XML "C:\Users\user\AppData\Local\Temp\tmp1EE6.tmp
Imagebase:	0x810000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6892 Parent PID: 6788

General

Start time:	18:03:48
Start date:	13/01/2022
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: RegSvcs.exe PID: 6956 Parent PID: 6280

General

Start time:	18:03:50
Start date:	13/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Imagebase:	0xc90000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.517211527.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.517211527.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.517211527.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.523432863.00000000059D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.523432863.00000000059D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.524096119.0000000005A70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.524096119.0000000005A70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.524096119.0000000005A70000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.522152896.00000000041A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.522152896.00000000041A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.285492337.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.285492337.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.285492337.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.287299484.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.287299484.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.287299484.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.286086026.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.286086026.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.286086026.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.286443560.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.286443560.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.286443560.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 2672 Parent PID: 6956

General

Start time:	18:03:57
Start date:	13/01/2022
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\tmp3840.tmp
Imagebase:	0x810000
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 — Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4352 Parent PID: 2672

General

Start time:	18:03:58
Start date:	13/01/2022
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: 3724 Parent PID: 6956

General

Start time:	18:04:00
Start date:	13/01/2022
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\tmp42FF.tmp
Imagebase:	0x810000
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 Show Windows behavior

File Read

Analysis Process: RegSvcs.exe PID: 476 Parent PID: 1104

General

Start time:	18:04:00
Start date:	13/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0
Imagebase:	0x570000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6400 Parent PID: 3724

General

Start time:	18:04:00
Start date:	13/01/2022
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: conhost.exe PID: 6408 Parent PID: 476

General

Start time:	18:04:00
Start date:	13/01/2022

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: 6636 Parent PID: 1104

General

Start time:	18:04:02
Start date:	13/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x660000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: conhost.exe PID: 6344 Parent PID: 6636

General

Start time:	18:04:03
Start date:	13/01/2022
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: 3748 Parent PID: 3292

General

Start time:	18:04:05
Start date:	13/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xb10000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6936 Parent PID: 3748

General

Start time:	18:04:06
Start date:	13/01/2022
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

Disassembly

Code Analysis