ID: 553323
Sample Name: 4jE4gfofqX.exe
Cookbook: default.jbs
Time: 17:03:16
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

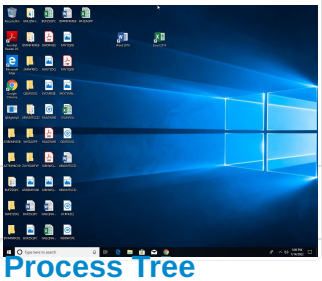
Windows Analysis Report 4jE4gfofqX.exe

Overview

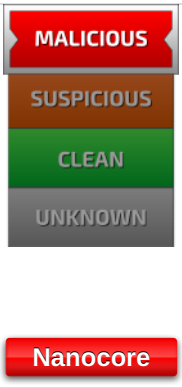
General Information

Sample Name:	4jE4gfofqX.exe
Analysis ID:	553323
MD5:	39924fd67ad38b4.
SHA1:	9d8af43fbfe30f21..
SHA256:	998746d0f5d0c13.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

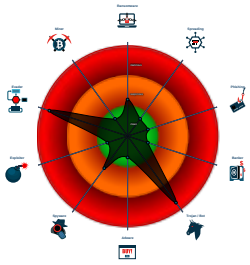


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- 4jE4gfofqX.exe (PID: 3080 cmdline: "C:\Users\user\Desktop\4jE4gfofqX.exe" MD5: 39924FD67AD38B45A9F0871798074EC4)
  - powershell.exe (PID: 6240 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\CGsmBdIfAlk.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 7160 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\CGsmBdIfAlk" /XML "C:\Users\user\AppData\Local\Temp\tmpC7DE.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5236 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 5684 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp20C3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6132 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp298E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6104 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 1324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6260 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5668 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "5ddb4cba-37cb-41bf-8dbf-b2a0e345",
  "Domain1": "nsayers4rm382.bounceme.net",
  "Domain2": "127.0.0.1",
  "Port": 2050,
  "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
00000000.00000002.688995010.00000000030B1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000007.00000003.701710687.0000000004865000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1ad2:$a: NanoCore • 0x1af7:$a: NanoCore • 0x1b50:$a: NanoCore • 0x11ced:$a: NanoCore • 0x11d13:$a: NanoCore • 0x11d6f:$a: NanoCore • 0x1ebc4:$a: NanoCore • 0x1ec1d:$a: NanoCore • 0x1ec50:$a: NanoCore • 0x1ee7c:$a: NanoCore • 0x1eef8:$a: NanoCore • 0x1f511:$a: NanoCore • 0x1f65a:$a: NanoCore • 0x1fb2e:$a: NanoCore • 0x1fe15:$a: NanoCore • 0x1fe2c:$a: NanoCore • 0x253ca:$a: NanoCore • 0x25444:$a: NanoCore • 0x29fe1:$a: NanoCore • 0x2b39b:$a: NanoCore • 0x2b3e5:$a: NanoCore
00000007.00000000.679409854.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000000.679409854.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.679409854.000000000040 2000.00000040.00000001.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
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.3.RegSvcs.exe.48881c5.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x3bd6:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
7.3.RegSvcs.exe.48881c5.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x605:$x2: NanoCore.ClientPluginHost • 0x3bd6:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x3cb4:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost • 0x3bf0:$s5: IClientLoggingHost
0.2.4jE4gfofqX.exe.42e7670.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.4jE4gfofqX.exe.42e7670.3.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
0.2.4jE4gfofqX.exe.42e7670.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 36 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

Antivirus detection for URL or domain

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

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:

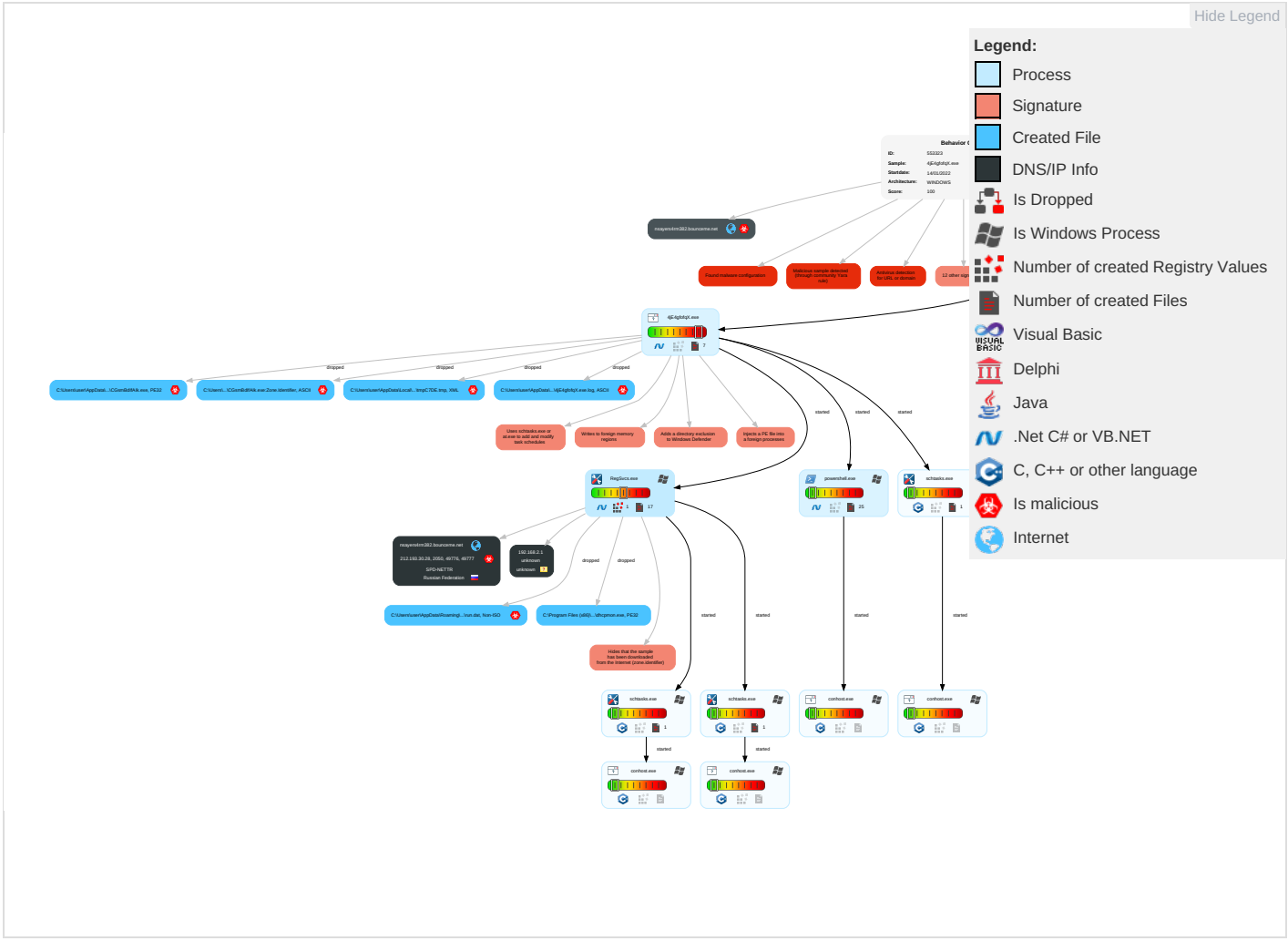
Detected Nanocore Rat

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 2 1 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explc Redir Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explc Track Local
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Mani Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

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
4jE4gfofqX.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CGsmBdIfAlk.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		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fonts.comc;MLD	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivau	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com6	0%	Avira URL Cloud	safe	
http://www.carterandcone.comams	0%	URL Reputation	safe	
http://www.sandoll.co.kr.	0%	Avira URL Cloud	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.tiro.comna	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgl	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sandoll.co.krdD	0%	Avira URL Cloud	safe	
http://www.carterandcone.com6	0%	Avira URL Cloud	safe	
http://www.tiro.comVM	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comCt	0%	Avira URL Cloud	safe	
http://www.carterandcone.com9	0%	URL Reputation	safe	
http://www.carterandcone.com8	0%	URL Reputation	safe	
http://www.fontbureau.com4	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comnew	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.carterandcone.comexce	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.comcooo	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comueed	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
nsayers4rm382.bounceme.net	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.comng-	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cni-f	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn6	0%	URL Reputation	safe	
http://www.founder.com.cn/cn8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.carterandcone.comona	0%	URL Reputation	safe	
http://www.sandoll.co.krmark	0%	Avira URL Cloud	safe	
http://www.fontbureau.comv	0%	URL Reputation	safe	
http://www.carterandcone.comcoF	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.galapagosdesign.com/$	0%	Avira URL Cloud	safe	
http://www.urwpp.de.v	0%	Avira URL Cloud	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.carterandcone.comcoJ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nsayers4rm382.bounceme.net	212.193.30.28	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
127.0.0.1	true	• Avira URL Cloud: safe	unknown
nsayers4rm382.bounceme.net	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.30.28	nsayers4rm382.bounceme.net	Russian Federation		57844	SPD-NETTR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553323
Start date:	14.01.2022
Start time:	17:03:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4jE4gfofqX.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:	30
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@21/22@18/2
EGA Information:	• Successful, ratio: 25%
HDC Information:	• Successful, ratio: 6.1% (good quality ratio 4.4%) • Quality average: 46% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 83% • 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
17:04:11	API Interceptor	1x Sleep call for process: 4jE4gfofqX.exe modified
17:04:18	API Interceptor	30x Sleep call for process: powershell.exe modified
17:04:25	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:04:26	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
17:04:28	API Interceptor	833x Sleep call for process: RegSvcs.exe modified
17:04:29	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(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\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k... .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\4jE4gfofqX.exe.log	
Process:	C:\Users\user\Desktop\4jE4gfofqX.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	659
Entropy (8bit):	5.2661344468761735
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U2U/N0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2U/Pz2T
MD5:	3C153E5BCCA87FF6E091634EE977299F
SHA1:	6DE85803E7FA00C03CE809243EB8162DF036430A
SHA-256:	F0705BDCE38ADB33CA8B414DDB85718985660BC73E0BE4439E0A94384A37797D
SHA-512:	54BDFFA72A0D4122B5B79B092D7E8C3213EB30AE2858188748E52ADD65ADE2F2F887892C06BB8ED790C19F1ED949176B9A9F0113679EF38B74387A189E6DC74
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Trans actions\aa840ffb0dd775d9eb8d66c8a8e8cdd9\System.Transactions.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74f ce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, 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):	22272
Entropy (8bit):	5.6028179508540195
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SSDEEP:	384:2tCDLG0vHVY1gG/SCaRnYS0nMjultI+v7Y9g9SJ3xOT1Ma7ZlbAV7lWwiZBDI+iN:lm1gEmYTMCIthf9cUCafwkVE
MD5:	8CD4C69E7735A00B8E656FE76E0C58CE
SHA1:	F00BF1617BDD92B97E01FC7B20F6AE643ED7E21C
SHA-256:	568FC21DD09C9AE03E7988BA06BD1951D18CE1215C9A7B632496AB34DC22C17E
SHA-512:	4BF9A4D8702E1F6C8997C1EE46A77E1E4B6C9519448E614B4908C694A885DB2F4E776156F5E4CB264E9E7ECB4F1A286D11138E5321DC87A2760BA5C26641C47A
Malicious:	false
Preview:	@...e.....y.....h.....X...I.....@.....H.....<@.^.L."My...:P..... .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_l2tajiaq.gs0.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_ocbsmtkp.ghy.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\tmp20C3.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E 2BD5
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp20C3.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\tmp298E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\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\Local\Temp\tmpC7DE.tmp	
Process:	C:\Users\user\Desktop\4jE4gfofqX.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.139234187632499
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaNxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTIv
MD5:	C9924CDB058AE4F5ED4B8AE833BEB87E
SHA1:	064062D7979E05C27A0D8398DA876D7203D7F1F6
SHA-256:	54F27E662692D9D4BA3B6891459A6E3E5467A16DA5C31F970B8BB9B97C405328
SHA-512:	2537A55087D464B1EB5E914BC3BBACFA08F666BEB74A9A999D9CF015CD225775FB32E70B4C8246FD298AF3F5C9A7577B88FC600356D1F8100A4EEDB48390AF93
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</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\CGsmBdIfAIk.exe	
Process:	C:\Users\user\Desktop\4jE4gfofqX.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	445952
Entropy (8bit):	7.8925106493683295
Encrypted:	false
SSDEEP:	12288:iUcPAwUnh8+ZujiTkUe4a7sSGRfjQ2q8hrTaK9GMoqC:Dcv07ZmiTrnkGRM2/GKGqC
MD5:	39924FD67AD38B45A9F0871798074EC4
SHA1:	9D8AF43FBFE30F21C5F0E147DDC211EFB67E71C6
SHA-256:	998746D0F5D0C13DF720F0BF3981D652C828EA64D64D2E16736A80123FB534AA
SHA-512:	A77D009F8AA88F6CD0BC428219075169B495A16417AA3768E9D5BE20635F5DD785DBFE1B7F23CC8B37E841FC4F354EA07157970487D4EC29600F6CA56A697A96
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Roaming\CGsmBdIfAIk.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....~.... .....@.. .....@..... .@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... . .....@..B.....`.....H.....]...m.....$.....".(....*....0..G.....E.....+ ~....+ ~....+.~....+.~....+.~....+..*..0.....E...%.r.. .p.%.r...p.%.r%..p.%.r7..p.....E...%.rI..p.%.r[..p.%.r%..p.%.r7..p.....E...%.r...p.%.rm..p.%.r...p.%.r...p.....E...%.r...p.%.r...p.%.r...p.%.r...p.....r...p.....E...%.rr..p.%.r.. .p.%.r...p.%.r...p.....*B.(.....}....*..0..1.....(.....(.....h5...b.&+...h;....8..

C:\Users\user\AppData\Roaming\CGsmBdIfAIk.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\4jE4gfofqX.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\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356 A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Ey:Ey
MD5:	DB32428FAED7BD0F8E9D84E5294DCA75
SHA1:	D840FF4CDF74027CE72EA3CE3954ACB9843E37AB
SHA-256:	DA6FA2B36D2081EBA6FB0AB2A094DA77942C12B77D72F6B4EF60AE2F6C990949
SHA-512:	46C91D972ED944BD18B2504325DA7EECFA5EF1D6F268B4F77431FF6E977C52F2FDE3F1892265928D4714ECB31B079E6EE5F8936CADA68972F404D7700D589684
Malicious:	**true**
Preview:	|.,.w..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.584962500721156
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBn:RzWDqTB
MD5:	3FCC766D28BFD974C68B38C27D0D7A9A
SHA1:	45ED19A78D9B79E46EDBFC3E3CA58E90423A676B

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
SHA-256:	39A25F1AB5099005A74CF04F3C61C3253CD9BDA73B85228B58B45AAA4E838641
SHA-512:	C7D47BDAABEEBB8C9D9B31CC4CE968EAF291771762FA022A2F55F9BA4838E71FDBD3F83792709E47509C5D94629D6D274CC933371DC01560D13016D944012D 5
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44 F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:....L.g<.....I..%4[.G^.~.l'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,...u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\Documents\20220114\PowerShell_transcript.105270.F8elBDBn.20220114170416.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):	5793
Entropy (8bit):	5.397620486346515
Encrypted:	false

C:\Users\user\Documents\20220114\PowerShell_transcript.105270.F8elBDBn.20220114170416.txt	
SSDEEP:	96:BZ4jVNqqDo1ZEZyjVNqqDo1ZXThrjZ0gjVNqqDo1ZeibbYZT:tC
MD5:	6DD6D9C7E7FE1FB610443D3993CD36A2
SHA1:	C09861D529FD1EF0A1CA5402DC478D528CB7650D
SHA-256:	F6BE896EB0BAE1A3217F39DE59EF00DBA13346EAFD4066F2BFC1F78F4F8B7198
SHA-512:	0FE3E12DF4F9CCB073E1E52B091DD285B7FC9DDC779B1DAF10C45C58BF682714BA0012B897076DC8F96E3F666829A76950654BEAD2DAB1184F3B6A38F24E4A 6
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114170417..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 105270 (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\CGsmBdIfAIk.exe..Process ID: 6240..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: 20220114170417..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppDa ta\Roaming\CGsmBdIfAIk.exe..**********..Windows PowerShell transcript start..Start time: 20220114170820..Username: computer\user..RunAs User: comput er\jo

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071B E
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [optio ns] AssemblyName..Options:... /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target app lication, 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... /rec onfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /no logo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	7.8925106493683295
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	4jE4gfofqX.exe
File size:	445952
MD5:	39924fd67ad38b45a9f0871798074ec4
SHA1:	9d8af43fbfe30f21c5f0e147ddc211efb67e71c6
SHA256:	998746d0f5d0c13df720f0bf3981d652c828ea64d64d2e1 6736a80123fb534aa
SHA512:	a77d009f8aa88f6cd0bc428219075169b495a16417aa376 8e9d5be20635f5dd785dbfe1b7f23cc8b37e841fc4f354ea 07157970487d4ec29600f6ca56a697a96
SSDEEP:	12288:iUcPAwUnh8+ZujiTkUe4a7sSGRfjQ2q8hrTaK9G MoqC:Dcv07ZmiTrnkGRM2/GKGqC
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... .a.....0.....~.... .....@.. .....@..... ...@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46e37e
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:	0x61E18ED8 [Fri Jan 14 14:55:20 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6c384	0x6c400	False	0.917842450924	data	7.90399867909	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x5e4	0x600	False	0.4296875	data	4.16236823097	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x72000	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
01/14/22-17:04:29.027612	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54531	8.8.8.8	192.168.2.4
01/14/22-17:04:42.016659	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53097	8.8.8.8	192.168.2.4
01/14/22-17:05:00.517356	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55854	8.8.8.8	192.168.2.4
01/14/22-17:05:26.047805	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.8.8	192.168.2.4
01/14/22-17:05:32.163170	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51255	8.8.8.8	192.168.2.4
01/14/22-17:05:50.086098	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55046	8.8.8.8	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-17:06:01.948967	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50601	8.8.8.8	192.168.2.4
01/14/22-17:06:13.810038	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59172	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 17:04:29.006839037 CET	192.168.2.4	8.8.8.8	0xecf1	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:35.225557089 CET	192.168.2.4	8.8.8.8	0x605f	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:41.995484114 CET	192.168.2.4	8.8.8.8	0x7dfe	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:48.019675016 CET	192.168.2.4	8.8.8.8	0xd8eb	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:54.246776104 CET	192.168.2.4	8.8.8.8	0xc8cb	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:00.495065928 CET	192.168.2.4	8.8.8.8	0x4aae	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:06.960705042 CET	192.168.2.4	8.8.8.8	0x4cb6	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:13.337006092 CET	192.168.2.4	8.8.8.8	0x3c2b	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:19.897420883 CET	192.168.2.4	8.8.8.8	0x4ecd	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:26.029577971 CET	192.168.2.4	8.8.8.8	0xd629	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:32.140371084 CET	192.168.2.4	8.8.8.8	0xb5c3	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:38.122148991 CET	192.168.2.4	8.8.8.8	0x6deb	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:44.172910929 CET	192.168.2.4	8.8.8.8	0x1f32	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:50.064846992 CET	192.168.2.4	8.8.8.8	0x65a5	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:55.985610962 CET	192.168.2.4	8.8.8.8	0x53f6	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:06:01.927673101 CET	192.168.2.4	8.8.8.8	0x798	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:06:07.878652096 CET	192.168.2.4	8.8.8.8	0xbfb7	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:06:13.789107084 CET	192.168.2.4	8.8.8.8	0x611	Standard query (0)	nsayers4rm382.bounceme.net	A (IP address)	IN (0x0001)

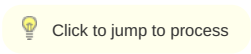
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 17:04:29.027611971 CET	8.8.8.8	192.168.2.4	0xecf1	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:35.244611025 CET	8.8.8.8	192.168.2.4	0x605f	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:42.016659021 CET	8.8.8.8	192.168.2.4	0x7dfe	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:48.039402962 CET	8.8.8.8	192.168.2.4	0xd8eb	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:04:54.266310930 CET	8.8.8.8	192.168.2.4	0xc8cb	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:00.517355919 CET	8.8.8.8	192.168.2.4	0x4aae	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:06.978233099 CET	8.8.8.8	192.168.2.4	0x4cb6	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:13.354682922 CET	8.8.8.8	192.168.2.4	0x3c2b	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:19.916755915 CET	8.8.8.8	192.168.2.4	0x4ecd	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:26.047805071 CET	8.8.8.8	192.168.2.4	0xd629	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:32.163170099 CET	8.8.8.8	192.168.2.4	0xb5c3	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:38.141475916 CET	8.8.8.8	192.168.2.4	0x6deb	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:44.192060947 CET	8.8.8.8	192.168.2.4	0x1f32	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:50.086097956 CET	8.8.8.8	192.168.2.4	0x65a5	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:05:56.004957914 CET	8.8.8.8	192.168.2.4	0x53f6	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:06:01.948966980 CET	8.8.8.8	192.168.2.4	0x798	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:06:07.898730040 CET	8.8.8.8	192.168.2.4	0xbfb7	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)
Jan 14, 2022 17:06:13.810038090 CET	8.8.8.8	192.168.2.4	0x611	No error (0)	nsayers4rm382.bounceme.net		212.193.30.28	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 4jE4gfofqX.exe PID: 3080 Parent PID: 6060

General

Start time:	17:04:05
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\4jE4gfofqX.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4jE4gfofqX.exe"
Imagebase:	0x950000
File size:	445952 bytes
MD5 hash:	39924FD67AD38B45A9F0871798074EC4
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: 00000000.00000002.688995010.00000000030B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.689772422.0000000004194000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.689772422.0000000004194000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.689772422.0000000004194000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.689265362.0000000003206000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6240 Parent PID: 3080

General

Start time:	17:04:15
Start date:	14/01/2022
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\CGsmBdIfAIk.exe
Imagebase:	0x120000
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: 7164 Parent PID: 6240

General

Start time:	17:04:16
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 7160 Parent PID: 3080

General

Start time:	17:04:16
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\CGsmBdIfAIk" /XML "C:\Users\user\AppData\Local\Temp\tmpC7DE.tmp
Imagebase:	0x12e0000
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: 6828 Parent PID: 7160

General

Start time:	17:04:17
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: RegSvcs.exe PID: 5236 Parent PID: 3080

General

Start time:	17:04:18
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xd90000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000007.00000003.701710687.0000000004865000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.679409854.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.679409854.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.679409854.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.681763573.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.681763573.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.681763573.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.679721715.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.679721715.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.679721715.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.681331500.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.681331500.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.681331500.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

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: 5684 Parent PID: 5236

General

Start time:	17:04:24
Start date:	14/01/2022
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\tmp20C3.tmp
Imagebase:	0x12e0000
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: 740 Parent PID: 5684

General

Start time:	17:04:25
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6132 Parent PID: 5236

General

Start time:	17:04:26
Start date:	14/01/2022
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\tmp298E.tmp
Imagebase:	0x12e0000
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: 6104 Parent PID: 968

General

Start time:	17:04:27
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0x5c0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5196 Parent PID: 6132

General

Start time:	17:04:27
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6eb840000
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: conhost.exe PID: 1324 Parent PID: 6104

General

Start time:	17:04:27
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6260 Parent PID: 968

General

Start time:	17:04:29
Start date:	14/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xe90000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
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: 6276 Parent PID: 6260

General

Start time:	17:04:29
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5668 Parent PID: 3424

General

Start time:	17:04:33
Start date:	14/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x7ff732050000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6452 Parent PID: 5668

General

Start time:	17:04:34
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis