ID: 798041
Sample Name:
004349256789197.pdf.scr.exe
Cookbook: default.jbs
Time: 17:50:31
Date: 03/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

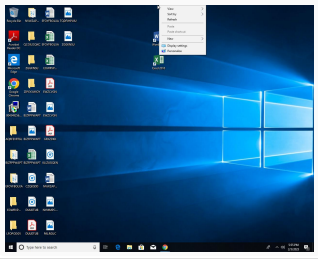
Windows Analysis Report

004349256789197.pdf.scr.exe

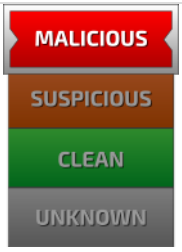
Overview

General Information

Sample Name:	004349256789197.pdf.scr.exe
Analysis ID:	798041
MD5:	3ac05bbe3529…
SHA1:	ee12d93ac5f81..
SHA256:	576263fb3c889..
Tags:	exe
Infos:	



Detection



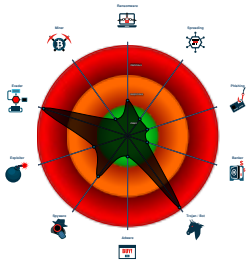
Nanocore

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

Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AntiVM autoit script
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Starts an encoded Visual Basic Scr…
- Creates multiple autostart registry k…
- Initial sample is a PE file and has a…

Classification



Process Tree

- **System is w10x64**
- 004349256789197.pdf.scr.exe (PID: 912 cmdline: C:\Users\user\Desktop\004349256789197.pdf.scr.exe MD5: 3AC05BBE35293FBFD0DF49ECFB34C461)
  - wscript.exe (PID: 5348 cmdline: "C:\Windows\System32\wscript.exe" laklj-aowdkfxknm.xml.vbe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - ihgsvw.exe (PID: 5624 cmdline: "C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe" ccmbpoh.docx MD5: 797174324A2A71F55AD4E89DA918B52D)
      - RegSvcs.exe (PID: 3008 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
        - schtasks.exe (PID: 4524 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpA401.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 4876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 5040 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpAA3C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 5116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - ihgsvw.exe (PID: 5040 cmdline: "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC MD5: 797174324A2A71F55AD4E89DA918B52D)
          - RegSvcs.exe (PID: 1724 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- RegSvcs.exe (PID: 3784 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 3956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ihgsvw.exe (PID: 2200 cmdline: "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC MD5: 797174324A2A71F55AD4E89DA918B52D)
  - RegSvcs.exe (PID: 2756 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 5176 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 2220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- wscript.exe (PID: 1840 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - ihgsvw.exe (PID: 5948 cmdline: "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC MD5: 797174324A2A71F55AD4E89DA918B52D)
    - RegSvcs.exe (PID: 2884 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 2344 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 3696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- wscript.exe (PID: 3384 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - ihgsvw.exe (PID: 2788 cmdline: "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC MD5: 797174324A2A71F55AD4E89DA918B52D)
    - RegSvcs.exe (PID: 5632 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- ihgsvw.exe (PID: 5648 cmdline: "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC MD5:

797174324A2A71F55AD4E89DA918B52D)
- RegSvcs.exe (PID: 4588 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)

- wscript.exe (PID: 5884 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - ihgsvw.exe (PID: 5304 cmdline: "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC MD5: 797174324A2A71F55AD4E89DA918B52D)
    - RegSvcs.exe (PID: 4768 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "d95e5ad5-6193-4689-a919-7befded6",
  "Group": "ITEego",
  "Domain1": "december2n.duckdns.org",
  "Domain2": "december2nd.ddns.net",
  "Port": 60705,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 29996,
  "MutexTimeout": 4996,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "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 Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xfcc5:$x1: NanoCore.ClientPluginHost • 0x2c465:$x1: NanoCore.ClientPluginHost • 0xfd02:$x2: IClientNetworkHost • 0x2c4a2:$x2: IClientNetworkHost • 0x13835:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x2ffd5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfa2d:$a: NanoCore • 0xfa3d:$a: NanoCore • 0xfc71:$a: NanoCore • 0xfc85:$a: NanoCore • 0xfcc5:$a: NanoCore • 0x2c1cd:$a: NanoCore • 0x2c1dd:$a: NanoCore • 0x2c411:$a: NanoCore • 0x2c425:$a: NanoCore • 0x2c465:$a: NanoCore • 0xfa8c:$b: ClientPlugin • 0xfc8e:$b: ClientPlugin • 0xfcce:$b: ClientPlugin • 0x2c22c:$b: ClientPlugin • 0x2c42e:$b: ClientPlugin • 0x2c46e:$b: ClientPlugin • 0xfbb3:$c: ProjectData • 0x2c353:$c: ProjectData • 0x105ba:$d: DESCrypto • 0x2cd5a:$d: DESCrypto • 0x17f86:$e: KeepAlive
00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xfcc5:$a1: NanoCore.ClientPluginHost • 0x2c465:$a1: NanoCore.ClientPluginHost • 0xfc85:$a2: NanoCore.ClientPlugin • 0x2c425:$a2: NanoCore.ClientPlugin • 0x11bde:$b1: get_BuilderSettings • 0x2e37e:$b1: get_BuilderSettings • 0xfae1:$b2: ClientLoaderForm.resources • 0x2c281:$b2: ClientLoaderForm.resources • 0x112fe:$b3: PluginCommand • 0x2da9e:$b3: PluginCommand • 0xfcb6:$b4: IClientAppHost • 0x2c456:$b4: IClientAppHost • 0x1a136:$b5: GetBlockHash • 0x368d6:$b5: GetBlockHash • 0x12236:$b6: AddHostEntry • 0x2e9d6:$b6: AddHostEntry • 0x15f29:$b7: LogClientException • 0x326c9:$b7: LogClientException • 0x121a3:$b8: PipeExists • 0x2e943:$b8: PipeExists • 0xfcef:$b9: IClientLoggingHost
00000011.00000003.353786178.0000000004299000.00000004.00000020.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xffad:$x1: NanoCore.ClientPluginHost • 0xffea:$x2: IClientNetworkHost • 0x13b1d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 258 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
29.3.ihgsvw.exe.133eea0.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
29.3.ihgsvw.exe.133eea0.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
29.3.ihgsvw.exe.133eea0.1.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
29.3.ihgsvw.exe.133eea0.1.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
29.3.ihgsvw.exe.133eea0.1.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 350 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Yara detected Nanocore RAT

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking

Uses dynamic DNS services

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Creates multiple autostart registry keys

Creates autostart registry keys with suspicious values (likely registry only malware)

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)

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion

Yara detected AntiVM autoit script

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

Found API chain indicative of sandbox detection

HIPS / PFW / Operating System Protection Evasion

Starts an encoded Visual Basic Script (VBE)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

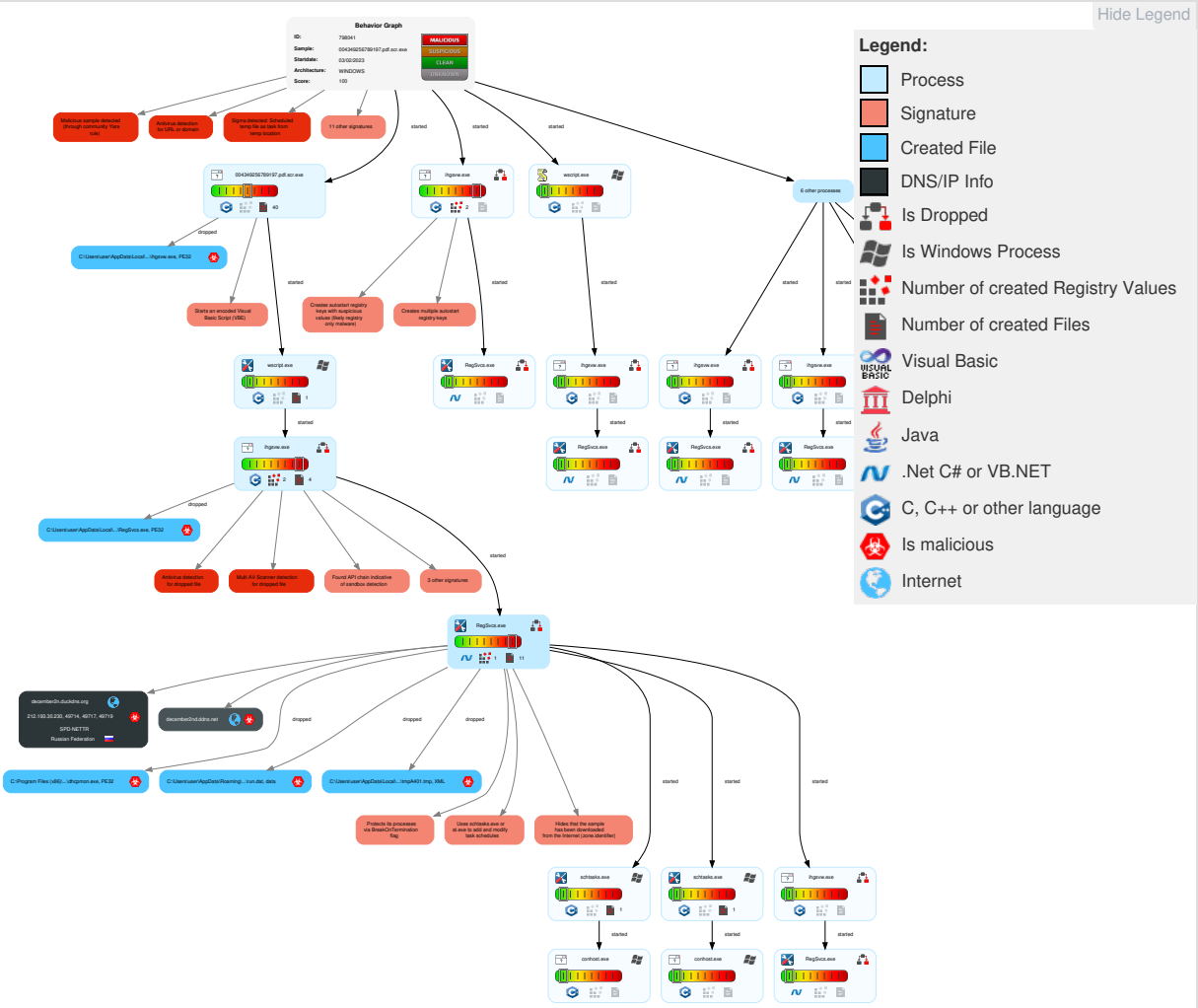
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 1 Scripting	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 1 Disable or Modify Tools	2 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Native API	1 Scheduled Task/Job	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	2 1 Registry Run Keys / Startup Folder	3 1 2 Process Injection	1 1 1 Scripting	Security Account Manager	4 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Data Encoding	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Scheduled Task/Job	Logon Script (Mac)	1 Scheduled Task/Job	1 2 Obfuscated Files or Information	NTDS	3 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	2 1 Registry Run Keys / Startup Folder	1 2 Software Packing	LSA Secrets	3 4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Masquerading	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	3 1 2 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

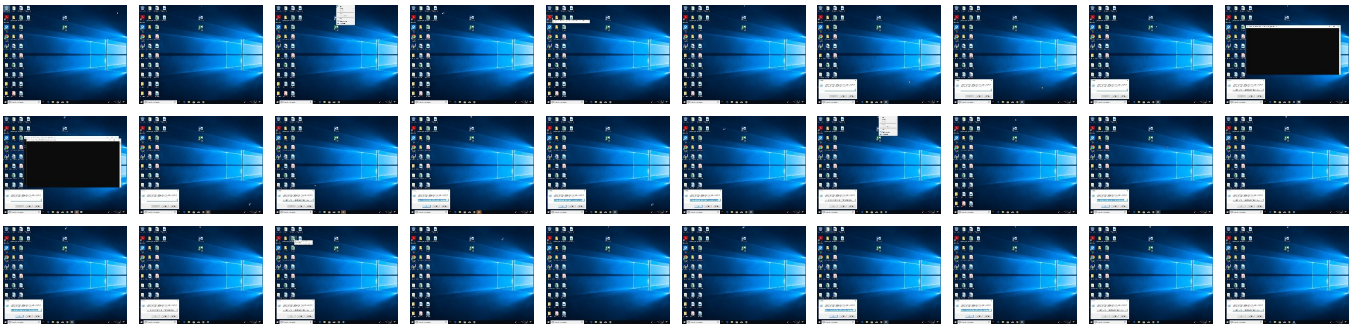
Behavior Graph

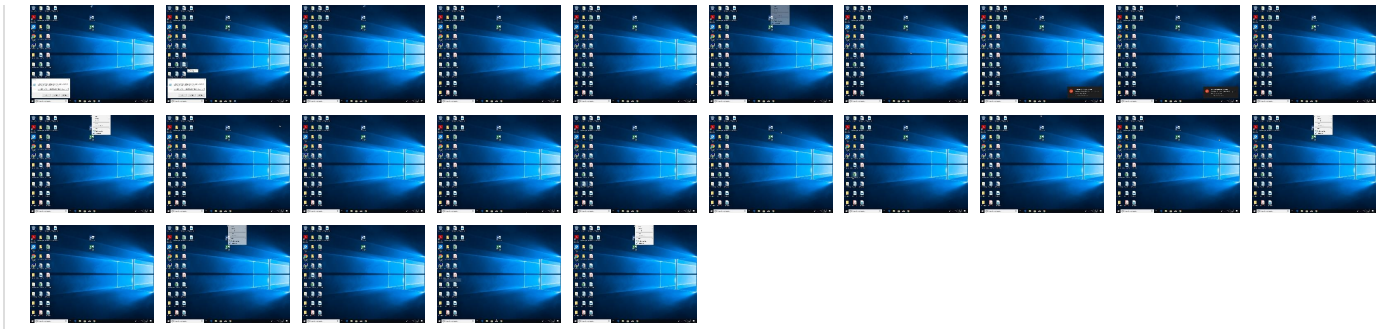


Screenshots

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
004349256789197.pdf.scr.exe	45%	ReversingLabs	Win32.Trojan.Lisk	
004349256789197.pdf.scr.exe	39%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe	100%	Avira	DR/AutoIt.Gen	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe	26%	ReversingLabs	Win32.Dropper.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.2.RegSvcs.exe.720000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.RegSvcs.exe.6210000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
december2nd.ddns.net	100%	Avira URL Cloud	malware	
december2n.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	212.193.30.230	true	true		unknown
december2n.duckdns.org	212.193.30.230	true	true		unknown

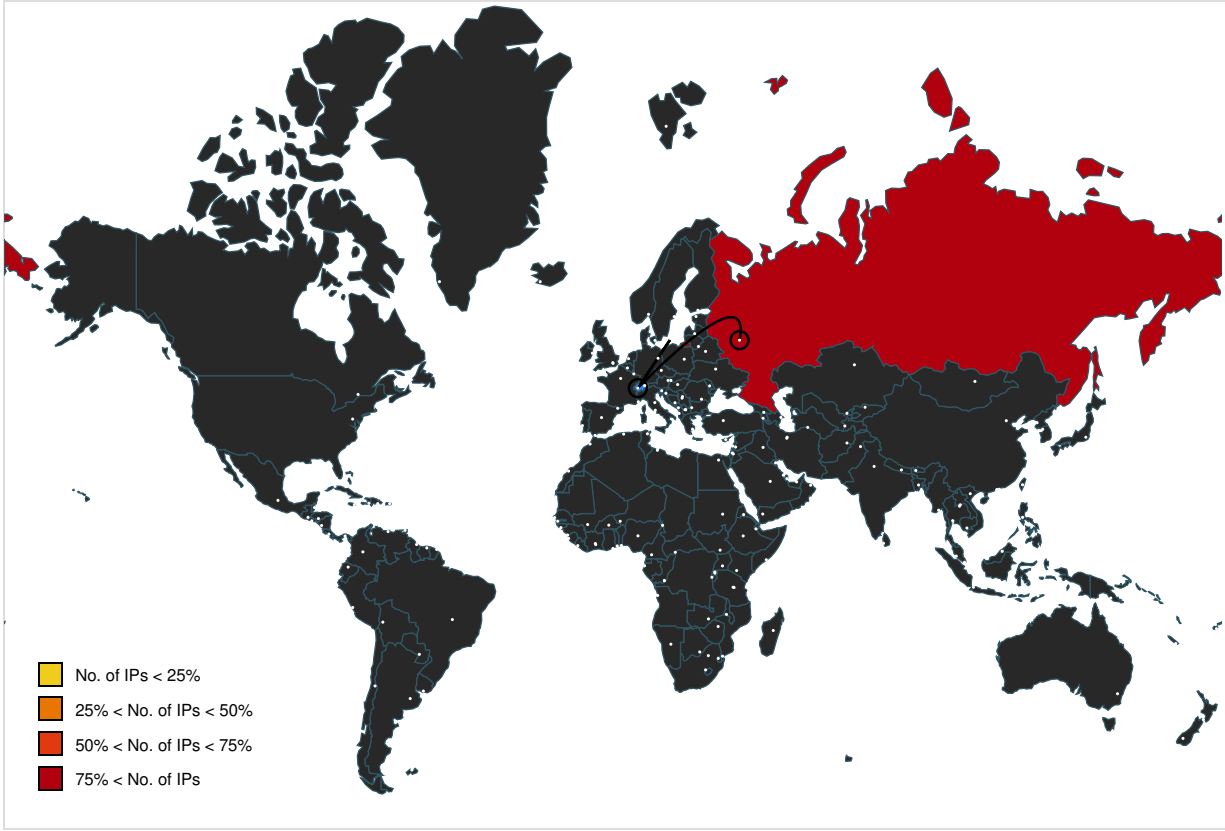
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	true	• Avira URL Cloud: malware	unknown
december2n.duckdns.org	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.autoitscript.com/autoit3/	004349256789197.pdf.scr.exe, 00000000.00000003.264105403.0000000006D09000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegSvcs.exe, 0000000A.00000002.774805901.0000000002C31000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.30.230	december2nd.ddns.net	Russian Federation		57844	SPD-NETTR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	798041
Start date and time:	2023-02-03 17:50:31 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	004349256789197.pdf.scr.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@43/45@28/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.7% (good quality ratio 92.4%) • Quality average: 78.8% • Quality standard deviation: 29.5%

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:51:58	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
17:52:03	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
17:52:06	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
17:52:06	API Interceptor	1646x Sleep call for process: RegSvcs.exe modified
17:52:06	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs
17:52:15	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:52:25	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
17:52:33	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs
17:52:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
17:52:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\AppData\Local\Temp\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+SdIBf0k2dsYyV6lq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WgIAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Reputation:	unknown
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\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WgIAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Reputation:	unknown
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\Temp\Folder10_51\Update.vbs

Process:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	151
Entropy (8bit):	5.088165235670747
Encrypted:	false
SSDEEP:	3:FER/n0eFH5OerbJSRE2J5xAIzbgDU4AdjNerbJSRE2J5xAIzbgRoeqn:FER/IFHIe0i23fzbgDUPjNe0i23fzbg2
MD5:	A9A3C2871C5B661CFE0BD95B12693457
SHA1:	E8C39E23AE2DF49D7D9C461BE91C20FF1B4FDB44
SHA-256:	C64E277FBBCB7B0B7693A0EA11925A1AB3C966723A97A2381851EE269DA571AF
SHA-512:	44B1D4E5CF629E6A91B32721B9B7E2939455DB0ACAEC08DE68E8512CB0C6503BE549E09C3E28E0EAFCB32812B72E398EF471FB39BDF3EF4E15AB3AF58BA63CDE
Malicious:	false
Reputation:	unknown
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC"

C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	data
Category:	dropped
Size (bytes):	121649618
Entropy (8bit):	7.0364100465274175
Encrypted:	false
SSDEEP:	196608:NFJK4YyNlildTiCgW6hwsT3mYfb4tMV6zlR5+gmtZtQJYuPng/Kj8nGj3AExAcYc:g
MD5:	004A5D8E43630E4D5DB63A5BB6159FCC
SHA1:	285BD4A523DC7B93B0EFB86978D0FA4591E45D85
SHA-256:	9D5D8B0428D63CC43A9503591D94C62CD1606C26732735A2A950CA63147B367B
SHA-512:	F7756E3FB6B82FB75C53B6CAB6BA5E97B7774ED61F41549E222038FB3C745BD2784FC85D8ECC4DAAD7F09139A73C8E44863BC07E226AF71B4292609774034CD4
Malicious:	false
Reputation:	unknown
Preview:	..;....?..li....A.m.....E.6...BO....12...R.g.&...T.......W...*D7.24.r....tE.....mX.IU.$..kX...........#.c.s..u.o[x..(+LK.z.....k....CmlV..=m..`r6.[.....2~9Y....I.5....%.0Ld.."YMT.....cEN1.. ..,..m!.j{...9d]..9..`j..Y....-.*.....w...]...v......5.3.H.9.7.3.x.5.8.4.4.1.b.O.5.Q.8.m.X.4.8.2.L.....m.s.A.q.C.q.W.4.6.Z.7.8.3.p.4.0.0.9.4.9.4.1.e.7.6.9.Q.3.1.2.5.E.0.3.1.1.3.4.w .2.1.e.Y.Q.y.u.h.5.......!....S.[.=G..di.~..e4Z...%...s..}9.Z..v.J..".:L.....OG.....`.4{[.UZld4..{c..Y...+...wp..gg<$.3.....M.K...P.x......h......G..x.E...Jat.....G....!.....!6.o..+...R|.X...#l.. 0. ..!..8.[.*.Y.......G....5.......r^...\{sH."..rKN.....4.1.9.N.4.e.n.d.0.0.h.V.9.C.3.6.4.s.2.T.5.2.9.9.S.3.9.7.p.g.1.7.8.J.8.2.7.Y.I.1.....'@.0...~@...`..i7.....&.h.+9yb[m....$...d0.-(.r ...ah'.@.....5.i.h.1.d.M.v.N.9.4.N.1.1.3.8.I.0.e.V.d.q.4.K.7.7.5.7.y.M.5.1.0.1.e.3.4.3.8.4.3.....f.K.aX,.D..Lo.+.Z.(6Z0r..!l.yu...0+z\...,...aK..R.....H.=5...o,C..}&n,.h..'..._y... o.#vOo.D.}|.....=.}.]..A...E

C:\Users\user\AppData\Local\Temp\Folder10_51\cdjr.ktl

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	407473
Entropy (8bit):	4.048588207938584
Encrypted:	false
SSDEEP:	
MD5:	48F9952AAAFE4CA15D39581E78889AC0
SHA1:	569F6FB010FEFB412192A968784DB355B8311853
SHA-256:	7F322D3E2096AA1F60CBF945595F155314D434A4FDD5A35640DF9363570FE666
SHA-512:	BAE18549694F7D75F24D057F21380C30CA6F9C7579EE3D4EAD2F4CAFF92E541797ABFA970688170501DE1EA378B5F0CAF071B46BD7C28030D6C15EFBA5296B87
Malicious:	false
Reputation:	unknown
Preview:	0x4D5*9--3---04---FFFF--_8-------4----------08----E/F_*0E-_409CD2/_80/4CCD2/546869732070726F67726/6D20636/6E6E6F742062652072756E20696E20444F53206D6F64652E0D0D0*24-------5045--4C0/03-*/27E954--------E--E0/0_0/06--C80/--7E0/-----92E70/--2-----2---4--02----2--04-------04--------*-3--02------02-----/--0/----0/----0/------0/----------038E70/-57----2-2-787*0/----------02-0C----------2---8----------082--048----------2E74657874---98C70/--2---0C80/--02-------2--0602E72656C6F63--0C-----02--02---C*0/----------4--0422E72737263---787*0/--2-2--7C0/--CC0/----------4--04----------074E70/-----48---02-05-E4D6--54/-/-03---CE0/-06CCC4--/8/2----------/33-3-5/---0/--//026F35--0*/82E02/62*026F36--0*/E2D0*2606/69//F0*2E332_030*2_F406/69/20*C---330E06/79//F0F3/0706/79//F2032/606/69/20C---0330*06/79/20*8---2E02/62*/72*---033-9-45-------7337--0*/92D28267338--0*/72D26267339--0*/62C242673

C:\Users\user\AppData\Local\Temp\Folder10_51\cfciwbpw.xl

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	588
Entropy (8bit):	6.213002454543603
Encrypted:	false
SSDEEP:	
MD5:	F821802654AA671984C34C52D1CDCFD4
SHA1:	D4E04EFDB9402CA2090A8602C54B84400ABC71A1
SHA-256:	4BB1B7DE0C409D831CE769B0ACB7ED9F753710B487D3B6135C5758DD0AAFD86C
SHA-512:	8DAB9616753F29F84BAA87012F6FEA6A0185DF12BCE18D334DFF95AC77210EF25680EAD8FC034F60D0EBB40B4D78FA814902F1EE49519E813E9A91FFE3F36AAB
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\crldjt.icm

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	6.2118134349266025
Encrypted:	false
SSDEEP:	
MD5:	046256AD551F6765F23E871E20A666A5
SHA1:	79FF6979F39E5DCFA15B81922E947B19B4A4D6B0
SHA-256:	08248EBE1BCE86EA542860C50CCD847580D22CB133A78D524B5D1C714CBBB331
SHA-512:	57BB2D43E8263F6B2F9D37A609940B7BB8B8A0C324451FAA78AD8A35264DA04D3461B58787C3632D7506D2F52D49032B20716FBB8060014FD098FE830F6820BA
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\dftbvs.bmp

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	607
Entropy (8bit):	6.201298305828523
Encrypted:	false
SSDEEP:	
MD5:	043E8B1857BEEABA3718A7F3847122D5
SHA1:	7BB750324587EDB34690AA0B789869B15406ECDD
SHA-256:	9524F0E243E06157AFAAD36B50DAF38166331029B5226C16543B2F7AEA1F4E2F
SHA-512:	D7F29E19A3162697D314DD98B3C11E1DDAE2768C79F7E25F96D36D38E5AC2FF0F15BB2DBE9A3F19AADF2430554865099B8F12C9B07C005C8E835CB16FFADA2FA
Malicious:	false
Reputation:	unknown
Preview:	.....6.....&.....

C:\Users\user\AppData\Local\Temp\Folder10_51\fkjavmq.jpg

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	6.206196757309823
Encrypted:	false
SSDEEP:	
MD5:	6E72ACECBCA63A02F17F09893C4ECC5B
SHA1:	B667E4B9DD2659CF40784B523AB6ECAFC715C452

SHA-256:	B6C25984BEEC32852E2AB5E928F7099DE75BAED20852749A603ED89EFC219E63
SHA-512:	E1CF9C9DAA24A5B4099AE18DDB4E6E9B572ED9251E13BE0D804D3A35E9F0171EB4420921CFAB625058744209D9E6604FC370F1B365CDB60ABFFCEF162E366458
Malicious:	false
Reputation:	unknown
Preview:	.....;

C:\Users\user\AppData\Local\Temp\Folder10_51\hvwq.msc

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	6.2074620354651575
Encrypted:	false
SSDEEP:	
MD5:	4BD4541ADFD4E488EACDFF04D29183BE
SHA1:	46FF43B901FE30FC60D07FD8F913BDB9B7C7756D
SHA-256:	0C5F56ABB0BC00576718A0554507D9068FB7E83E4E3B44FE5435371467AD160C
SHA-512:	58E109BC252B51DE3770B5062759158E359D47E51682E66D9E693585BB64E3425D54D3DB4EB3D95B43AE6B2D18F724480594885A363D29CE6DCC9C27436B613F
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\igkuh.pdf

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	669
Entropy (8bit):	6.256842582335099
Encrypted:	false
SSDEEP:	
MD5:	D20C31B84E18489E4E27B1D5591E9F45
SHA1:	7F6D3CD2F26E1E458C91FA23BB2E489737A6286D
SHA-256:	A8E5BE91B492A1B25ED40D3C9BF20B9CACF662B6C15180A77BF3033C073C292E
SHA-512:	549140F915E92F090AD58571EB544E7D18AB6E4E0D2BEABAF036D95884B12E3FD547474DBF8F793E7691D4D9F1709CF333C41E3D73FFB29791B174D1EF3A122
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1357068
Entropy (8bit):	6.400387425104881
Encrypted:	false
SSDEEP:	
MD5:	797174324A2A71F55AD4E89DA918B52D
SHA1:	0B75AD2A9E182993A220D261F74B68D70F97398A
SHA-256:	AED1188582A5A13FF39A6C9D324BC9A5D0A8CEDB56814B1017CC35D2A6F3548E
SHA-512:	F9A1799F74EF31AB2958463D9557AD3A65D51112F90EC64674DD5675115997019248F5C920E8DEB50A12A90BA2A6EF40D2C5F00C98B3ABD4D3E081866F37B7F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..h..h..hX;1h..hX;3hq..hX;2h..hr..h..h...i...h...i...h...i...h..Ch..h..Sh..h..h..hI..i...hI..i..hI.?h..h.Wh..hI..i..hRich..h.....PE..L...).(c.....".....@.....@...@.....@.....@.....@.....|....P..4.....~..X&...`..Pv.....C.....@.....text...|..... ..`.rdata.....@..@.data...lp.....H.....@....rsrc...4....P.....@..@.reloc..Pv...`...x.....@..B.....

C:\Users\user\AppData\Local\Temp\Folder10_51\itgtrnq.icm	
Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	578
Entropy (8bit):	6.208581968969855
Encrypted:	false
SSDEEP:	
MD5:	18D244E2DA84E8B08621DB3D2C714ECE
SHA1:	7C03348C271C40E02418075E5678A5906576C280
SHA-256:	592477758051ED96DBCF1300248BD10B1F800287D7E0AFD8012A7D4B446E4C91
SHA-512:	671FEA619563C02F32E0458CE15062BE3F9404A795F763EDEB2934CA0DA24B5487AE721D9CA1B4A5B056E8FB1B8684EF45F7E90519DD6EBF4C90143E01A628E5
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\jdcefmmt.exe	
Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	701
Entropy (8bit):	6.217263929891554
Encrypted:	false
SSDEEP:	
MD5:	03224F8D3517549E40641731A5211E8D
SHA1:	C9FC0CCFAB73A464DABE64D52737D86ED47DE581
SHA-256:	9FA367942F2C23664CBC8498A334C716F26BF2C1732A5C9490876CBAA3944F6E
SHA-512:	B0E1BE6303B1BB5426F9F0F40AF342544CDD393783F87108B63C5216FAB128FE5AB25561515CECAEE0FA1572A5C8227B08C49E11E18ECFDC08E58A653DE9A743
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\jvhiixkk.ini	
Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	6.213056313966432
Encrypted:	false
SSDEEP:	
MD5:	9FFFAA49E0C74C82366B031E8D873414
SHA1:	B71020F66B4D55066C04A5504425649B93DC78F2
SHA-256:	251A281F2856F3CFEC0FD3472028E9ED3AEB5EF558CCAC820EA67C9E8524FE6A
SHA-512:	3E103990CFD5057E9D9B9095805227B226DA59DA4974E237046D1D98653E3C67629DC74C6C0647FFE0A9E8EFAE2F4999E1C2C9EFB2B5C8081879D895CC9A41AA
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\kcvtlxr.xml	
Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	620
Entropy (8bit):	6.222206344450024
Encrypted:	false

SSDEEP:	
MD5:	DDC613AF180A41E7B305D2D26E77AED6
SHA1:	682E34C9A6D1A245798B44BE73D47399CBFC60A3
SHA-256:	A0B85CAEE9398B79BB9D7BE632FC2CA14A4E53204A8ECCA296C8CF25C9BAC7F4
SHA-512:	B6A7931AC3281005313641C9D1C3472E4E4646BC63A7B559A6CA911ACD959CF9D07B802E8F919F8DDAA995E61F0B9DEB57BA3C21EE9886D03360C6B1E905E0B
Malicious:	false
Reputation:	unknown
Preview:	.....B.....

C:\Users\user\AppData\Local\Temp\Folder10_51\kjwnj.pdf

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	6.245326274571603
Encrypted:	false
SSDEEP:	
MD5:	A70B8C03B325053D2F0A2051E3D566B7
SHA1:	E1A9CB6F876034FCD418A94D1A201DFE26631399
SHA-256:	CA9CD4CDD48DFFDDE0F6418CD08766E00E842634CC615D636540ED30CFD3C433
SHA-512:	8C5F1A8DF42EE671DE09C3D86F1B579B424C4D78E719EF96EE2B88B07DA04FAA1F0F92CDCDE4B4A25A616BD0F6F134A8636C5701E78D3747CBAA9A5F901E2B8B
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\laklj-aowdkfxknm.xml.vbe

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	46328
Entropy (8bit):	7.200808834838652
Encrypted:	false
SSDEEP:	
MD5:	E3A50ED6D88E9A241C5F8A38C74B75A5
SHA1:	DF2C2FAA8BB5C3D9B14D9A8CDBBF7E86F4F5034A
SHA-256:	E65F26F6FDABF467EE52D7466856CC152B9ECC355596FEBB34E5910413A2CD6D
SHA-512:	4714A1F10420EA1BED67ABA05B4D1E45D48D2BC2944CCCA93F1CB5F7B32F23147D869B6865E4B0A5D703D1F886C650907A4633EBDE9455A84BCC8065DEA18C77
Malicious:	false
Reputation:	unknown
Preview:	..'..9..3....h.>...}....] .....].o.RG^....n?Z.h=.k.([._.....H..Q..7.4.].x..c.?..k...dd..Qp` ....i.>..d..........@o.?~.z.x.....'.Z.c.c.h.c.B.9.5.4.N.9.p.c.9.9.E.8.9.w.V.E.6.r.3.2.1.Y.4.3.Q.5.d.9.4.8.0.9.2.X.5.4.S.x.1.7.B.A.y.W.w.....'.4.Z.6.8.1.5.X.4.9.Y.F.2.6.S.8.M.C.8.8.2.1.p.z.1.7.9.....'....R).....s....Q..*.;..G.o.Sb....6...$.{r7Z.....@..TK..5).....GnS.&k.o...F..h.P..+.\|.....f^J..(m....._.5....$....b8!n...M..R..~{...Q..#\....T..e.yJ...I.....W[@...r..F*.Z.....ipr....'.w.A.U.3.C.4.0.a.h.o.J.1.A.W.0.8.2.D.e.I.S.8.N.4.0.6.J.2.1.5.U.C.V.1.0.s.8.U.L.G.7.1.8.i.K.C.0.....'.5.X.w.z.0.2.W.3.y.R.4.h.3.W.n.M.1.S.a.3.3.k.X.6.J.S.A.t.....'.6.4.i.8.L.T.I.8.a.7.i.D.4.8.U.0.n.5.V.7.b.s.e.g.1.....'..Q./.....nA*.._U.-..t.:+.H.Yeq.(.....E..Pg....LI.....K.@AkY..% ".....n.4K@'.'...K....MC.|..I.Y.f.....z8.Z.G<!....'.J.....[.....v..%TKerW~...J..J2YP.m|...N].IN.....g....Py....4."<%.U..+.._.L..t.I.....r..B.6.B....v?/.F.....a....~=.e....W":.....K.T...bkB,...9k#y

C:\Users\user\AppData\Local\Temp\Folder10_51\lpolln.ini

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	632
Entropy (8bit):	6.226044296719832
Encrypted:	false
SSDEEP:	
MD5:	32C554BAC7052BFF5BBB4E69058154E4
SHA1:	A46476E21653B14423F462D7C3CF6EC16199A204
SHA-256:	B4BFAAF128F118F5B45AAEDC20246B3517926363C75DA64EBEF63D648FCBAC08

SHA-512:	D74B0DEDAC5A006E06CE5A9D7F91C1AC4FE5E4D355EC7A9F8F8683CDB83D4E584A47937D8B3C58198FC85A4C2F14261953B527E79204A53E64C3F6B9B3FB51BD
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\Folder10_51\mttapgts.dll

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	535
Entropy (8bit):	6.223028920694769
Encrypted:	false
SSDEEP:	
MD5:	C32315E0688E0A5633A0D2DCE4CC9629
SHA1:	F581EE1E102167C604CF366415105BB9314CF4B5
SHA-256:	E92602D9F89967C956CA83477F419BF1F5F917D95E3C0501BD6EA1BF76E85808
SHA-512:	F5FFC31716F87A024883845607BE750FF782F114C3EC76378F6A78255857A47C9929EBDDBC9325CBE1D35887FAED615F1874320326C40215EFBE2A99193E2BF4
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\nkbixmwpld.ppt

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	6.264380029804187
Encrypted:	false
SSDEEP:	
MD5:	194DE31777DD53F9E29A06776AE6C1B3
SHA1:	A4FF9EF9C4962628810B38368D4EFB13F53449D7
SHA-256:	90EA34BF2E24E4AD5DF9FD37CEA36ABB7784931028F401F98A2E6C2A10B5583E
SHA-512:	637EAED24EB4EF8A4EE96BFAF11524901799DC8FBFD2DFDB3B478521B99BE49D056A9745388AC29A70A54390A449FC493B6F9CA5E00095DBDB192FA236B1C9B1
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\opmotkfi.msc

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	584
Entropy (8bit):	6.2507180834396046
Encrypted:	false
SSDEEP:	
MD5:	F87E4604F5916FF6A25186B0B504E681
SHA1:	DB2989E8ED40A5CEED078473341C5D8B8FE4E0F7
SHA-256:	0A8B1D99032C6B90054E5ADF89EFA61D005B0F3E12DA48905051067ED906D529
SHA-512:	9CDD4285C8B9CF1C90BD9A73071C839D933EE44149E8CE689AA1ADE39056EAFD9CBBF348AC8BD5340A2DF7E8D91AE0529E872C377FA90DE46FB698395A8D9152
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\riviu.pdf

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators

Category:	dropped
Size (bytes):	733
Entropy (8bit):	6.231676397919319
Encrypted:	false
SSDEEP:	
MD5:	DD66397E376C91D7F01F231D944C8DF1
SHA1:	8C2F651AF93B763090395AED51C2E551942DFEC3
SHA-256:	FF281486360AD0A5E071BFAE276626E80D212EA65AFBD3CA7784B0F4B3570D09
SHA-512:	7E81472C48AF0D9712068FB66500253F673629A313AF680071E8C8C961CB27D589F249AD688292259E384E4BCFC48161E901C6CB27659E16B42242C1E1CF2238
Malicious:	false
Reputation:	unknown
Preview:	.....%.....

C:\Users\user\AppData\Local\Temp\Folder10_51\rjfwh.icm

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	6.220144182081156
Encrypted:	false
SSDEEP:	
MD5:	7FFF06723AFA9FC84547B1E2D379AABD
SHA1:	4929D1A9298E365087EFDD2B019C05F6CF750E70
SHA-256:	B26D7992C99861FEE8E8E86614AF8A0B145AE8F2AEA197CE6BA8408EF07B9698
SHA-512:	538759223E6C9DEFE1F50B1AFF4C44CDDAF21C0712C51271E44431683C6E7F632F57800909CB48B7A0C26A02DDE11549FD996DFEDE8B50C97731CCB77B24EAB
Malicious:	false
Reputation:	unknown
Preview:	.....*.....

C:\Users\user\AppData\Local\Temp\Folder10_51\sdhmdt.msc

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	581
Entropy (8bit):	6.223635486991566
Encrypted:	false
SSDEEP:	
MD5:	B74B8AC3F96B39CC953D1BA34CB751DD
SHA1:	48050CB8EA9C5A3B5108706C987799673A1454FC
SHA-256:	A3FB7C9084245E0939340B7ABBFA54C7AE7367CCF3D5E134EAA847E1EA453AEC
SHA-512:	A7F912456131E21627C14DADD6DF84AA9642006191D60A7E0B486B3850B8B0B63F87C559C5257344C98917501289782DFFC9347670B265C908CFDAEB0CDCCAE
Malicious:	false
Reputation:	unknown
Preview:	.....j.....

C:\Users\user\AppData\Local\Temp\Folder10_51\taon.jpg

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	501
Entropy (8bit):	6.190656898709683
Encrypted:	false
SSDEEP:	
MD5:	4171BED3F16A92882815F61417AB975A
SHA1:	97A4483C79036BE8148C6169C7CCFF080742F40C
SHA-256:	E5F2CF9586AA8F0634FEE2474D46BCF6030846F0B4A02FED80F65700FCA8F0F8
SHA-512:	59566FBFDF44FE734293BF1E1DC1FAC5A63D4458E858EA05B602F56613257F99DEEBB4C7D961169A01C774DAC87A1BA35C020B7FB9FF327970E60973661A109
Malicious:	false

Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\tuhvewrqqk.xml

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	514
Entropy (8bit):	6.214291435583763
Encrypted:	false
SSDEEP:	
MD5:	55F643ECFE99B550B4823D0DB2E473C1
SHA1:	1DE1E7E890127FBCE7DCC4283B1F0ED2073071B8
SHA-256:	3283E76A48819F103CA6F2E58AB9911EF46DA4A6438E9CD37FD0628E0F664E17
SHA-512:	02B7C643A796B8B88CA0E3EE20024E15F13E0BB25B1A08F331408D0405EE39A478728365D61FC722356F73058050FD2230C28600076A8DCFCADEAC9BE1066863
Malicious:	false
Reputation:	unknown
Preview:	.....P.....

C:\Users\user\AppData\Local\Temp\Folder10_51\usvv.dll

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	6.170181324269657
Encrypted:	false
SSDEEP:	
MD5:	42788E9A82626033D1C890FEC1616027
SHA1:	4BC3D32071130B8830BA6999CAB6E836AFA741A6
SHA-256:	60B95B214023625539B917062F51833E9923711321185E7702ECCF0F9E16B256
SHA-512:	0334DB3EDE8EA3CB5107527EE5F162EFA37CE7C4CDBB168361614A6300443C0BDCF03590340C0E985882DA20C66717CC585F8621758AA81A9953BA04BA7ACCB
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\utxniv.icm

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	583
Entropy (8bit):	6.261328591888464
Encrypted:	false
SSDEEP:	
MD5:	E5450ED1310BAA27DF96331533B7116A
SHA1:	8F6F7C76A308B213EF39DE070CD3DF23B90EC209
SHA-256:	B5A1C32F1B74BD9BC40CB515B88DD0B1C0FB449DABC9E93AC75C581F111EEFB3
SHA-512:	519BE0EAFDBCD915E4C404F11DA4A713364BDF2EB4A2ADAD0E0CC16E3B0AA634C5AD0A5F498CCE8E3193365BDE1635154F054B4D54E4BF47EA6ACBA6F041A459
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\uvoxoq.jpg

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	753

Entropy (8bit):	6.265094025870397
Encrypted:	false
SSDEEP:	
MD5:	61F20CA5A3C48D6323D19BEB700DE2F4
SHA1:	FEC46018E797396868619396016CC00F3E9F0D7D
SHA-256:	8637DDC34CC6276D56738F219D8AD4EB4BBF73D80CEE16AA0C686B96E49031A2
SHA-512:	AD6CABC216D4F5212FC3AA7EDAD6289E6CBE4C6E7336E804083D0E8AB390F6554E088B735761A6F3E1D7D9F93737EA0D2E32FB02B7ECD787EF6F5BDC49840 4A
Malicious:	false
Reputation:	unknown
Preview:	.....f.....

C:\Users\user\AppData\Local\Temp\Folder10_51\vkeewq.txt

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	6.201022804655084
Encrypted:	false
SSDEEP:	
MD5:	3D1A20AE25ACA76918F525813753BB90
SHA1:	40EF954835A5E919E13155803E422FCB59A4D6E7
SHA-256:	72B7AA6124893C2A087D1691D2C7AD052903E028BEE451F5350C7BFFA2C50AD5
SHA-512:	706116CECE24D60C06B4691FF94B01BB7811165D6003CD7829CD32C9F791DEB2FC30753E9FEE794A1947CB422BCA69E7A5E6C90C8BCC07FA7598C579D185AD D3
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\vlsdwgv.docx

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	6.227023728555456
Encrypted:	false
SSDEEP:	
MD5:	BF8C92BF8491E4783B72B4CCDA5E91BB
SHA1:	7D3E0FE500A79523FCB5C9E636E3B399C0FD8CA9
SHA-256:	B7FDCD17F59F82AD25996F0D1DB018624A51022D94780493A4AB98047C2EA7A3
SHA-512:	42092933F616ED495EE9D2DB9C5C40C34DA55DFE9E9A74A832DED06106EE0BF142AE220780BE2E820C97878A6B88BAFF450B66C89966D02F73F659974BD7A3E F
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\wfccrina.ini

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	34981
Entropy (8bit):	5.585572477462829
Encrypted:	false
SSDEEP:	
MD5:	923021E60F76E22DF3997015A75D2DE2
SHA1:	0BF1F4312CB742E0FD3AA4797CD68839DD50EB86
SHA-256:	AC7EB1744189B9B145C3056E7847B5C17F27ED32BB66E05C5B7AE5CA024866B3
SHA-512:	C9E2B8BD11CF6DC78AF257148ABF0E0126FFE55130E6A80F63DEB33FA320B7048C6AFADDFEB692BD5D747D47D0EAD7EB45B203E62BB4F085567AB7E3E5032 00B
Malicious:	false

Reputation:	unknown
Preview:	oL0826i1j1u..0f8r26zx431oHqN82gD145xd6x0E8YWVM650gXWc0rm8V095vib1Vsg1ph8EKi5D7y..0173r5904j1898hnZJb026fa4507MCD53T3vXl2e2hbl70s9i 3zLKNVc5p3xW22..vn1x706pd349Btai6yHA162L25q1UP68785556E35xTBkR10GQ34sD9KF685..Mzu91s391IX01TMyJx7274d68P3gcZjpy8K953..THq58775p06y PBeXyG02646wz345m9..s99120P1V9hdVZ3clCMqTD28Of780zY4DzQ37cN134g91N686gb482862..4i8uy6nx2A2M54dp79IL4G13clh3V02K96F56zVemX8..W7687B 9MDnbR9vwrauSB6VulPly512506f5cfUC95D6277z44oQa7693845g52AVt3..0u2yc89702DWG392FlgnM8ffH6KdQ0A..jbmz085IBt5747RXzqI96174BEbEg3FCq97 V39DTc75b6E776P5Lv658L..78718M9c92LxuBRb1d6k..6L7d8elyRl47L0K3hOHKb7k4I70T0A3l9zv22464RI..6K1Vi3jmT54uR8nrL1dc3w068ZH4rw6L9..Pg8qe yhfwbbcBAp51Wap0PsJET4909M3Vb6R39EMbyM3B5h8ye1q6V1..8ZA5K6d89Y18oh2rx3f98oWa23O2RIx0qErnm6489d9n9kq6Fj79t3O79uKm7541..Xi640jzRer6E 56F83Va2B6uq39s5Ygif1oQY48J7hJ59331174QK265544201w9uNUm0gy0Zulw9..2X94fc65x4j53AD7A50N27n3Znl164U25O18689190M78a2lK..7FP81La529Q70 2RX0e8w02950u2V6UfP85Fr9U5uv48U183T2U90W79UL10o860dF2q264..o1JI2X27358f15m9M8..195dc62uVyg

C:\Users\user\AppData\Local\Temp\Folder10_51\whonujk.xml

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	6.245277588351939
Encrypted:	false
SSDEEP:	
MD5:	6A372892797F0436A2022B5C0D051DDF
SHA1:	D2138DA84C4D4469393DAF6B309C699D3776835B
SHA-256:	7E732B89FD4BA6996C2FEFB7DB6DA5BDE6B85E6BC44F7EA21DAA62992AE6A61A
SHA-512:	F25D9D07788FCB898C9174F06CFD76FC86F5CDD1202463BFA431CD7DCF72BD4B3616D3EF6F1B373898E551B515771F2A8DF8ED7E199982B0BC89AB06C0C401 1
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder10_51\wuqc.docx

Process:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	704
Entropy (8bit):	6.242209133425222
Encrypted:	false
SSDEEP:	
MD5:	30766DEDBDECAFF845571EEA5F3B21E4
SHA1:	514644B945925EEEE525AF9A8737277954B89288
SHA-256:	084034C5553C3DC615FA87DD84E10679480C16460B6A7F2EF3C5D8B0943683DD
SHA-512:	9CA41F1331CDBDE97DFFE697D3500117AB4DB8D19A12A900910CF8AF0526CEF5311295E10B3464FAA1451B3F6C8E445B8C48360FDDF239DAEF5E4651B76D6E 0
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\RegSvcs.exe

Process:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D 6B42
Malicious:	**true**
Reputation:	unknown

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\Temp\tmpA401.tmp

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1311
Entropy (8bit):	5.120237537969728
Encrypted:	false
SSDEEP:	
MD5:	9CC9B31561289BF47DDBEF114BE4B6FA
SHA1:	C901987D5F8BBAD7231B7EE4A65ADB93BB0F56A5
SHA-256:	984AA44429B06B17C290376A8D741A2DAE62FE6F38EEBBF434A0781230686097
SHA-512:	075F148FDD9187FDD6BA56D1CD3D81641FE8D8F9FBA903F98B307463B4BCDC77556B542CFD73C9BC2C34D364245D5B8080DE69DC968DE9070D44FE180741D4C
Malicious:	**true**
Reputation:	unknown
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\tmpAA3C.tmp

Process:	C:\Users\user\AppData\Local\Temp\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:	
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	51BBBB873C030E460FAD17FEDABBC3AB
SHA1:	5CC4E4B44A56143A4634286AA9E05F8607426C06
SHA-256:	AF3FBBF96097D55438E4F0F623AB560923B3E01927AC132EEA4D194DF8D96F42
SHA-512:	FAB50F156C07AF56AD56024C5E3E9443F1E31A524EAE3EA50BA699AC7CDEF7EE8BA65219E2A10F24F42D025C1080787F847CDE081FD21D10649D86B89516AB8B

Malicious:	**true**
Reputation:	unknown
Preview:	Y.;hR..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.556127542695029
Encrypted:	false
SSDEEP:	
MD5:	71C86F4534ED6EA4C1E9A785F2EB0A92
SHA1:	D065F0540580FC2E0ACD365784FD5A60F8235829
SHA-256:	DBC475B81DC4AACF70235516B8FB463D4FB170C3E72E647C0BA2A30D3B9EC4E3
SHA-512:	6D97D624C0A2B3D3B8D51A4F2502B8874E59E29538AD0477F1DE32FEEDAE38890F68532B591EEF0FA0DB23CD4929890DB256ACB8E4B73F6F790BB11C1347368
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\wfccrina.ini

Process:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	91
Entropy (8bit):	5.006199003780079
Encrypted:	false
SSDEEP:	
MD5:	AEF559A1D83E37D78B012A94CCE85889
SHA1:	44228F31FBDA6D787CD91E082E8EF769A23B37AA
SHA-256:	637F2CAB19C58F9E961062E379089A4DCDDCA806EA439BC8C0E63285DEC9F294
SHA-512:	235B7E78EBFFC6640E9476A85C3FD528A4C420F62DCA2AD7FA8C8105669B3278DEDBD50E51B73A7344775C7B9C076594DFDC91FD3857875278066039B91D9A9
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%localappdata%\temp..Key=Chrome..Dir3ctory=Folder10_51..ExE_c=ihgsvw.exe..

\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:	
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Reputation:	unknown
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, for MS Windows
Entropy (8bit):	7.853911292117169
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	004349256789197.pdf.scr.exe
File size:	1181640
MD5:	3ac05bbe35293fbfd0df49ecfb34c461
SHA1:	ee12d93ac5f81036e920bb8c05638aa4e6c1f3bf
SHA256:	576263fb3c88934ebdb0aa6071f3a980710c9dfd2a3d63d09b0aa76f1caac9e7
SHA512:	21f616118075066eda343383aad8d6f2dd71bc33c9b8efec3eedc891414d96a0602449abddb96513d55da97ddedb987d612d8227dfd8f64ca85ed2051eb02e14
SSDEEP:	24576:9TbBv5rUeTM/TYaxVKPijgGjFwJ5gRn0Bz76hZYBA3pUd26P207:XBvsHB7jQ5Cnq7+ZEA3pEt+0
TLSH:	AD451202BBC695B3D5A3193256753B11BA3CB9601FA58ECFA7E00A5CDA315C0DB317B2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x_c.<>..<>..<>.....1>.....>.....$>...l..>>...l../>...l..+>...l...>..5F..7>..5F..;>..<>..)?...l...>...l..=>...l..=>...l..=>.

File Icon

Icon Hash:	938c8c90b2ea6ab2

Static PE Info

General

Entrypoint:	0x41f530
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x6220BF8D [Thu Mar 3 13:15:57 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	12e12319f1029ec4f8fcbed7e82df162

Entrypoint Preview

Instruction
call 00007F216C70BF2Bh
jmp 00007F216C70B83Dh
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]

Instruction
mov esi, ecx
call 00007F216C6FE687h
mov dword ptr [esi], 004356D0h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 004356D8h
mov dword ptr [ecx], 004356D0h
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 004356B8h
push eax
call 00007F216C70ECCFh
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007F216C70B9CCh
push 0000000Ch
push esi
call 00007F216C70AF89h
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F216C6FE602h
push 0043BEF0h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F216C70E789h
int3
push ebp
mov ebp, esp
sub esp, 0Ch

Instruction
lea ecx, dword ptr [ebp-0Ch]
call 00007F216C70B948h
push 0043C0F4h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F216C70E76Ch
int3
jmp 00007F216C710207h
int3
int3
int3
int3
push 00422900h
push dword ptr fs:[00000000h]

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3d070	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3d0a4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x64000	0x4a8c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x69000	0x233c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3b11c	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x355f8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x278	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3c5ec	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x31bdc	0x31c00	False	0.5909380888819096	data	6.712962136932442	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0xaec0	0xb000	False	0.4579190340909091	data	5.261605615899847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x24720	0x1000	False	0.451416015625	data	4.387459135575936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x63000	0x190	0x200	False	0.4453125	data	3.3327310103022305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x64000	0x4a8c	0x4c00	False	0.6105571546052632	data	6.391160230365552	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x69000	0x233c	0x2400	False	0.7749565972222222	data	6.623012966548067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x64524	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6506c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x66618	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192		
RT_DIALOG	0x66740	0x286	data	English	United States
RT_DIALOG	0x669c8	0x13a	data	English	United States
RT_DIALOG	0x66b04	0xec	data	English	United States
RT_DIALOG	0x66bf0	0x12e	data	English	United States
RT_DIALOG	0x66d20	0x338	data	English	United States
RT_DIALOG	0x67058	0x252	data	English	United States
RT_STRING	0x672ac	0x1e2	data	English	United States
RT_STRING	0x67490	0x1cc	data	English	United States
RT_STRING	0x6765c	0x1b8	data	English	United States
RT_STRING	0x67814	0x146	data	English	United States
RT_STRING	0x6795c	0x46c	data	English	United States
RT_STRING	0x67dc8	0x166	data	English	United States
RT_STRING	0x67f30	0x152	data	English	United States
RT_STRING	0x68084	0x10a	data	English	United States
RT_STRING	0x68190	0xbc	data	English	United States
RT_STRING	0x6824c	0xd6	data	English	United States
RT_GROUP_ICON	0x68324	0x14	data		
RT_MANIFEST	0x68338	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

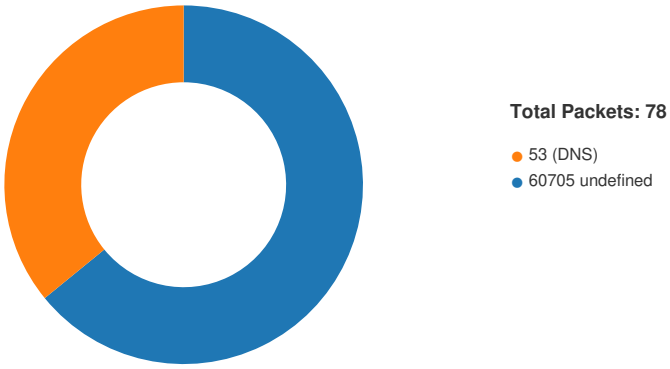
DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, InterlockedDecrement, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, DecodePointer, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, LocalFree, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage
OLEAUT32.dll	SysAllocString, SysFreeString, VariantClear
gdiplus.dll	GdipAlloc, GdipDisposeImage, GdipCloneImage, GdipCreateBitmapFromStream, GdipCreateBitmapFromStreamICM, GdipCreateHBITMAPFromBitmap, GdiplusStartup, GdiplusShutdown, GdipFree

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 17:52:09.616486073 CET	49714	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:10.228163958 CET	60705	49714	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:10.918013096 CET	49714	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:11.253858089 CET	60705	49714	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:11.918045998 CET	49714	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:12.473380089 CET	60705	49714	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:16.750894070 CET	49717	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:17.593020916 CET	60705	49717	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:18.106157064 CET	49717	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:18.553436995 CET	60705	49717	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:19.215564966 CET	49717	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:20.013190031 CET	60705	49717	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:25.434919119 CET	49719	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:25.738920927 CET	60705	49719	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:26.325540066 CET	49719	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:26.978645086 CET	60705	49719	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:27.521703959 CET	49719	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:28.055362940 CET	60705	49719	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:32.305283070 CET	49721	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:32.739506006 CET	60705	49721	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:33.393497944 CET	49721	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:33.869709015 CET	60705	49721	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:34.419946909 CET	49721	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:34.984946966 CET	60705	49721	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:39.125330925 CET	49723	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:39.763123989 CET	60705	49723	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:40.264465094 CET	49723	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:41.218107939 CET	60705	49723	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:41.733109951 CET	49723	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:42.393220901 CET	60705	49723	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:46.811115026 CET	49724	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:47.348661900 CET	60705	49724	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:48.015109062 CET	49724	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:48.524660110 CET	60705	49724	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:49.124406099 CET	49724	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:49.670073032 CET	60705	49724	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:53.803543091 CET	49726	60705	192.168.2.7	212.193.30.230

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 17:52:54.358467102 CET	60705	49726	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:54.921699047 CET	49726	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:55.728024006 CET	60705	49726	212.193.30.230	192.168.2.7
Feb 3, 2023 17:52:56.421844959 CET	49726	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:52:56.953017950 CET	60705	49726	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:02.842880964 CET	49727	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:03.413187027 CET	60705	49727	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:04.016222954 CET	49727	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:04.482964993 CET	60705	49727	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:05.125746012 CET	49727	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:05.448577881 CET	60705	49727	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:09.617194891 CET	49728	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:10.073801041 CET	60705	49728	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:10.642218113 CET	49728	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:11.048384905 CET	60705	49728	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:11.735630035 CET	49728	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:12.313384056 CET	60705	49728	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:16.493644953 CET	49730	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:16.968214989 CET	60705	49730	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:17.517337084 CET	49730	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:18.348334074 CET	60705	49730	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:18.874224901 CET	49730	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:19.189841986 CET	60705	49730	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:23.937660933 CET	49731	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:24.764730930 CET	60705	49731	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:25.361829042 CET	49731	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:25.743491888 CET	60705	49731	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:26.346234083 CET	49731	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:26.543648958 CET	60705	49731	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:30.786456108 CET	49732	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:31.345398903 CET	60705	49732	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:31.846702099 CET	49732	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:32.373364925 CET	60705	49732	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:32.878211975 CET	49732	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:33.493311882 CET	60705	49732	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:40.529577017 CET	49734	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:40.953541994 CET	60705	49734	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:41.644464970 CET	49734	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:42.034797907 CET	60705	49734	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:42.535142899 CET	49734	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:43.121236086 CET	60705	49734	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:47.350707054 CET	49735	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:47.818212032 CET	60705	49735	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:48.332509041 CET	49735	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:48.823368073 CET	60705	49735	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:49.332571030 CET	49735	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:49.707901955 CET	60705	49735	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:53.955672979 CET	49736	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:54.679156065 CET	60705	49736	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:55.192996025 CET	49736	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:55.649688959 CET	60705	49736	212.193.30.230	192.168.2.7
Feb 3, 2023 17:53:56.162882090 CET	49736	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:53:56.823153973 CET	60705	49736	212.193.30.230	192.168.2.7
Feb 3, 2023 17:54:01.482918978 CET	49737	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:54:01.823270082 CET	60705	49737	212.193.30.230	192.168.2.7
Feb 3, 2023 17:54:02.524898052 CET	49737	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:54:02.957899094 CET	60705	49737	212.193.30.230	192.168.2.7
Feb 3, 2023 17:54:03.462488890 CET	49737	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:54:04.038110971 CET	60705	49737	212.193.30.230	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 17:54:08.468101025 CET	49738	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:54:08.993590117 CET	60705	49738	212.193.30.230	192.168.2.7
Feb 3, 2023 17:54:09.509828091 CET	49738	60705	192.168.2.7	212.193.30.230
Feb 3, 2023 17:54:09.914083004 CET	60705	49738	212.193.30.230	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 17:52:09.443150997 CET	50835	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:52:09.550913095 CET	53	50835	8.8.8.8	192.168.2.7
Feb 3, 2023 17:52:16.610014915 CET	63926	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:52:16.726582050 CET	53	63926	8.8.8.8	192.168.2.7
Feb 3, 2023 17:52:25.314857960 CET	51007	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:52:25.424727917 CET	53	51007	8.8.8.8	192.168.2.7
Feb 3, 2023 17:52:32.281383038 CET	60765	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:52:32.303405046 CET	53	60765	8.8.8.8	192.168.2.7
Feb 3, 2023 17:52:39.102504015 CET	50024	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:52:39.124073029 CET	53	50024	8.8.8.8	192.168.2.7
Feb 3, 2023 17:52:46.786912918 CET	49516	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:52:46.806299925 CET	53	49516	8.8.8.8	192.168.2.7
Feb 3, 2023 17:52:53.769855976 CET	61392	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:52:53.789580107 CET	53	61392	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:02.823585987 CET	52104	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:02.841408968 CET	53	52104	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:09.590004921 CET	65356	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:09.609643936 CET	53	65356	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:16.469430923 CET	51526	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:16.487303972 CET	53	51526	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:23.915457010 CET	51139	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:23.933341980 CET	53	51139	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:30.759666920 CET	58784	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:30.779515982 CET	53	58784	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:40.419250965 CET	64608	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:40.527806997 CET	53	64608	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:47.239336967 CET	58746	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:47.348970890 CET	53	58746	8.8.8.8	192.168.2.7
Feb 3, 2023 17:53:53.936758995 CET	62433	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:53:53.954144955 CET	53	62433	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:01.462042093 CET	61248	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:01.481538057 CET	53	61248	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:08.436933994 CET	52750	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:08.458302975 CET	53	52750	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:15.322606087 CET	50231	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:15.342376947 CET	53	50231	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:22.567852020 CET	58514	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:22.587543011 CET	53	58514	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:29.466197014 CET	51436	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:29.579541922 CET	53	51436	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:36.820679903 CET	59053	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:36.838251114 CET	53	59053	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:44.068591118 CET	51945	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:44.086455107 CET	53	51945	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:50.906075954 CET	63187	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:50.928325891 CET	53	63187	8.8.8.8	192.168.2.7
Feb 3, 2023 17:54:57.821435928 CET	64760	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:54:57.844635010 CET	53	64760	8.8.8.8	192.168.2.7
Feb 3, 2023 17:55:05.101567984 CET	53637	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:55:05.210943937 CET	53	53637	8.8.8.8	192.168.2.7
Feb 3, 2023 17:55:13.758878946 CET	58343	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 17:55:13.865463018 CET	53	58343	8.8.8.8	192.168.2.7
Feb 3, 2023 17:55:20.557543993 CET	62018	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:55:20.577339888 CET	53	62018	8.8.8.8	192.168.2.7
Feb 3, 2023 17:55:27.259848118 CET	50155	53	192.168.2.7	8.8.8.8
Feb 3, 2023 17:55:27.279320955 CET	53	50155	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 3, 2023 17:52:09.443150997 CET	192.168.2.7	8.8.8.8	0xebe5	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:16.610014915 CET	192.168.2.7	8.8.8.8	0x5828	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:25.314857960 CET	192.168.2.7	8.8.8.8	0x3e16	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:32.281383038 CET	192.168.2.7	8.8.8.8	0x5585	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:39.102504015 CET	192.168.2.7	8.8.8.8	0x1074	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:46.786912918 CET	192.168.2.7	8.8.8.8	0xc899	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:53.769855976 CET	192.168.2.7	8.8.8.8	0x1b1f	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:02.823585987 CET	192.168.2.7	8.8.8.8	0x4c8e	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:09.590004921 CET	192.168.2.7	8.8.8.8	0x2d8c	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:16.469430923 CET	192.168.2.7	8.8.8.8	0x8848	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:23.915457010 CET	192.168.2.7	8.8.8.8	0x297b	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:30.759666920 CET	192.168.2.7	8.8.8.8	0xc6ec	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:40.419250965 CET	192.168.2.7	8.8.8.8	0xda46	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:47.239336967 CET	192.168.2.7	8.8.8.8	0xa48	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:53.936758995 CET	192.168.2.7	8.8.8.8	0x13d7	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:01.462042093 CET	192.168.2.7	8.8.8.8	0xfc42	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:08.436933994 CET	192.168.2.7	8.8.8.8	0x3b17	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:15.322606087 CET	192.168.2.7	8.8.8.8	0x4790	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:22.567852020 CET	192.168.2.7	8.8.8.8	0x2a56	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:29.466197014 CET	192.168.2.7	8.8.8.8	0xb3ae	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:36.820679903 CET	192.168.2.7	8.8.8.8	0x62ad	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:44.068591118 CET	192.168.2.7	8.8.8.8	0x2ae6	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:50.906075954 CET	192.168.2.7	8.8.8.8	0x9387	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:57.821435928 CET	192.168.2.7	8.8.8.8	0xfa40	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:55:05.101567984 CET	192.168.2.7	8.8.8.8	0x1982	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:55:13.758878946 CET	192.168.2.7	8.8.8.8	0xb7d7	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:55:20.557543993 CET	192.168.2.7	8.8.8.8	0x53ec	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:55:27.259848118 CET	192.168.2.7	8.8.8.8	0x4cb8	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false

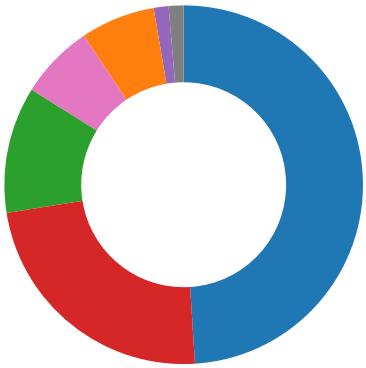
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 3, 2023 17:52:09.550913095 CET	8.8.8.8	192.168.2.7	0xebe5	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:16.726582050 CET	8.8.8.8	192.168.2.7	0x5828	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:25.424727917 CET	8.8.8.8	192.168.2.7	0x3e16	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:32.303405046 CET	8.8.8.8	192.168.2.7	0x5585	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:39.124073029 CET	8.8.8.8	192.168.2.7	0x1074	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:46.806299925 CET	8.8.8.8	192.168.2.7	0xc899	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:52:53.789580107 CET	8.8.8.8	192.168.2.7	0x1b1f	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:02.841408968 CET	8.8.8.8	192.168.2.7	0x4c8e	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:09.609643936 CET	8.8.8.8	192.168.2.7	0x2d8c	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:16.487303972 CET	8.8.8.8	192.168.2.7	0x8848	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:23.933341980 CET	8.8.8.8	192.168.2.7	0x297b	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:30.779515982 CET	8.8.8.8	192.168.2.7	0xc6ec	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:40.527806997 CET	8.8.8.8	192.168.2.7	0xda46	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:47.348970890 CET	8.8.8.8	192.168.2.7	0xa48	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:53:53.954144955 CET	8.8.8.8	192.168.2.7	0x13d7	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:01.481538057 CET	8.8.8.8	192.168.2.7	0xfc42	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:08.458302975 CET	8.8.8.8	192.168.2.7	0x3b17	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:15.342376947 CET	8.8.8.8	192.168.2.7	0x4790	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:22.587543011 CET	8.8.8.8	192.168.2.7	0x2a56	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:29.579541922 CET	8.8.8.8	192.168.2.7	0xb3ae	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:36.838251114 CET	8.8.8.8	192.168.2.7	0x62ad	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:44.086455107 CET	8.8.8.8	192.168.2.7	0x2ae6	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:50.928325891 CET	8.8.8.8	192.168.2.7	0x9387	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:54:57.844635010 CET	8.8.8.8	192.168.2.7	0xfa40	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:55:05.210943937 CET	8.8.8.8	192.168.2.7	0x1982	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 3, 2023 17:55:13.865463018 CET	8.8.8.8	192.168.2.7	0xb7d7	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:55:20.577339888 CET	8.8.8.8	192.168.2.7	0x53ec	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 3, 2023 17:55:27.279320955 CET	8.8.8.8	192.168.2.7	0x4cb8	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false

Statistics

Behavior



- 004349256789197.pdf.scr.exe
- wscript.exe
- ihgsvw.exe
- RegSvcs.exe
- schtasks.exe
- conhost.exe
- RegSvcs.exe
- schtasks.exe
- conhost.exe
- conhost.exe
- ihgsvw.exe
- dhcpmon.exe
- conhost.exe
- wscript.exe
- ihgsvw.exe
- RegSvcs.exe
- dhcpmon.exe
- conhost.exe
- RegSvcs.exe
- ihgsvw.exe
- wscript.exe
- RegSvcs.exe
- ihgsvw.exe
- RegSvcs.exe
- ihgsvw.exe
- wscript.exe
- ihgsvw.exe
- RegSvcs.exe
- RegSvcs.exe

Click to jump to process

System Behavior

Analysis Process: 004349256789197.pdf.scr.exe PID: 912, Parent PID: 3320

General

Target ID:	0
Start time:	17:51:27
Start date:	03/02/2023
Path:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\004349256789197.pdf.scr.exe
Imagebase:	0x3d0000
File size:	1181640 bytes
MD5 hash:	3AC05BBE35293FBFD0DF49ECFB34C461
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: wscript.exe PID: **5348**, Parent PID: **912**

General

Target ID:	1
Start time:	17:51:39
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\wscript.exe" laklj-aowdkfxknm.xml.vbe
Imagebase:	0xd10000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ihgsvw.exe PID: **5624**, Parent PID: **5348**

General

Target ID:	6
Start time:	17:51:49
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe" ccmbpoh.docx
Imagebase:	0xba0000
File size:	1357068 bytes
MD5 hash:	797174324A2A71F55AD4E89DA918B52D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.309488610.000000000182E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.309488610.000000000182E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.309488610.000000000182E000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.309488610.000000000182E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.311176660.00000000017F8000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.311176660.00000000017F8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.311176660.00000000017F8000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.311176660.00000000017F8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.309754638.0000000001861000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.309754638.0000000001861000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.309754638.0000000001861000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.309754638.0000000001861000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.309384867.00000000017F9000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.309384867.00000000017F9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.309384867.00000000017F9000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.309384867.00000000017F9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.310273116.000000000184C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.310273116.000000000184C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.310273116.000000000184C000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.310273116.000000000184C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.310180487.0000000001831000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.310180487.0000000001831000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.310180487.0000000001831000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.310180487.0000000001831000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.311013911.0000000004448000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.311013911.0000000004448000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.311013911.0000000004448000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.311013911.0000000004448000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.310685382.00000000017C5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.310685382.00000000017C5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.310685382.00000000017C5000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.310685382.00000000017C5000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 26%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	C0DADF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Folder10_51\Update.vbs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	BE59A8	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	C0DA78	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Folder10_51\Update.vbs	0	151	43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 2e 52 75 6e 20 22 43 3a 5c 55 73 65 72 73 5c 46 52 4f 4e 54 44 7e 31 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 46 4f 4c 44 45 52 7e 31 5c 69 68 67 73 76 77 2e 65 78 65 20 43 3a 5c 55 73 65 72 73 5c 46 52 4f 4e 54 44 7e 31 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 46 4f 4c 44 45 52 7e 31 5c 43 43 4d 42 50 4f 7e 31 2e 44 4f 43 22	CreateObject("WScript.Shell").Run "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC"	success or wait	1	C0D4EC	WriteFile
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	C0DA78	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx	unknown	65536	success or wait	1858	BD93D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx	unknown	12288	end of file	2	BD93D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx	unknown	65536	success or wait	1858	BD93D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx	unknown	12288	end of file	2	BD93D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx	unknown	65536	success or wait	1	BAB0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx	unknown	65536	success or wait	1813	BAB0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\ccmbpoh.docx	unknown	65536	end of file	1	BAB0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\Update.vbs	unknown	65536	end of file	1	BAB0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\cdjr.ktl	unknown	65536	success or wait	2	BAB0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder10_51\cdjr.ktl	unknown	65536	success or wait	14	BAB0B2	ReadFile

Registry Activities

Analysis Process: RegSvcs.exe PID: **3008**, Parent PID: **5624**

General

Target ID:	10
Start time:	17:51:58
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x360000
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.00000002.785005873.0000000006210000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.785005873.0000000006210000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.785005873.0000000006210000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.785005873.0000000006210000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.785005873.0000000006210000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.784950885.0000000006200000.00000004.00000001.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.784950885.0000000006200000.00000004.00000001.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.784950885.0000000006200000.00000004.00000001.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.784950885.0000000006200000.00000004.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.784420113.00000000052D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.784420113.00000000052D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.784420113.00000000052D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.784420113.00000000052D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.774805901.0000000002C31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.774805901.0000000002C31000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E3CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E3CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C81E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C8BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71C8DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71C87038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpAA3C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71C87038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C8BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	success or wait	1	71C86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpAA3C.tmp	success or wait	1	71C86A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	59 fd 3b 68 52 06 fd 48	Y;hRH	success or wait	1	71C81B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	71C8DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	0	1311	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	71C81B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	48	43 3a 5c 55 73 65 72 73 5c 46 52 4f 4e 54 44 7e 31 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe	success or wait	1	71C81B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpAA3C.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	71C81B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72DFD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72DFD72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	4096	success or wait	1	72DFD72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	512	success or wait	1	72DFD72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	71C8646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **4524**, Parent PID: **3008**

General

Target ID:	11
Start time:	17:52:02
Start date:	03/02/2023
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\tmpA401.tmp
Imagebase:	0xef0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	unknown	2	success or wait	1	EFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	unknown	1312	success or wait	1	EFABD9	ReadFile

Analysis Process: conhost.exe PID: **4876**, Parent PID: **4524**

General

Target ID:	12
Start time:	17:52:02
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **3784**, Parent PID: **1100**

General

Target ID:	13
Start time:	17:52:03
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0x10000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7314C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71C81B4F	WriteFile
\Device\ConDrv	141	141	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a 31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	The following installation error occurred:1: Assembly not found: '0'.	success or wait	1	71C81B4F	WriteFile
\Device\ConDrv	186	45	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'.	success or wait	1	71C81B4F	WriteFile
\Device\ConDrv	215	29	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71C81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	0	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	7314C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile

Analysis Process: schtasks.exe PID: **5040**, Parent PID: **3008**

General

Target ID:	14
Start time:	17:52:03
Start date:	03/02/2023
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\tmpAA3C.tmp
Imagebase:	0xef0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAA3C.tmp	unknown	2	success or wait	1	EFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAA3C.tmp	unknown	1311	success or wait	1	EFABD9	ReadFile

Analysis Process: conhost.exe PID: **3956**, Parent PID: **3784**

General

Target ID:	15
Start time:	17:52:04
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6edaf0000
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: **5116**, Parent PID: **5040**

General	
Target ID:	16
Start time:	17:52:04
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ihgsvw.exe PID: **2200**, Parent PID: **3320**

General	
Target ID:	17
Start time:	17:52:06
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
Imagebase:	0xba0000
File size:	1357068 bytes
MD5 hash:	797174324A2A71F55AD4E89DA918B52D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.352579534.0000000001962000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.353786178.0000000004299000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.353786178.0000000004299000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.353786178.0000000004299000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.353786178.0000000004299000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.351627736.000000000192A000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.351627736.000000000192A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.351627736.000000000192A000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.351627736.000000000192A000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.352185052.0000000001992000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.352185052.0000000001992000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.352185052.0000000001992000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.352185052.0000000001992000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.352676374.000000000197E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.352676374.000000000197E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.352676374.000000000197E000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.352676374.000000000197E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.354054231.0000000001929000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.354054231.0000000001929000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.354054231.0000000001929000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.354054231.0000000001929000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.353086726.00000000018F5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.353086726.00000000018F5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.353086726.00000000018F5000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.353086726.00000000018F5000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000003.351714814.000000000195E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000003.351714814.000000000195E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000003.351714814.000000000195E000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000003.351714814.000000000195E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: dhcpmon.exe PID: **5176**, Parent PID: **1100**

General

Target ID:	18
Start time:	17:52:07
Start date:	03/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x710000
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%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7314C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71C81B4F	WriteFile
\Device\ConDrv	141	141	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a 31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	The following installation error occurred:1: Assembly not found: '0'.	success or wait	1	71C81B4F	WriteFile
\Device\ConDrv	186	45	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'.	success or wait	1	71C81B4F	WriteFile
\Device\ConDrv	215	29	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71C81B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	7314C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile

Analysis Process: conhost.exe PID: **2220**, Parent PID: **5176**

General	
Target ID:	19
Start time:	17:52:07
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **1840**, Parent PID: **3320**

General	
Target ID:	20
Start time:	17:52:15
Start date:	03/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs"
Imagebase:	0x7ff6f21c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ihgsvw.exe PID: **5948**, Parent PID: **1840**

General	
Target ID:	21
Start time:	17:52:16
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
Imagebase:	0xba0000
File size:	1357068 bytes
MD5 hash:	797174324A2A71F55AD4E89DA918B52D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.373949530.0000000000EFB000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.373949530.0000000000EFB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.373949530.0000000000EFB000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.373949530.0000000000EFB000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.375313756.0000000003637000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.375313756.0000000003637000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.375313756.0000000003637000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.375313756.0000000003637000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.375626664.0000000000EC6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.375626664.0000000000EC6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.375626664.0000000000EC6000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.375626664.0000000000EC6000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.374648689.0000000000F1B000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.374648689.0000000000F1B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.374648689.0000000000F1B000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.374648689.0000000000F1B000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.374247545.0000000000F2F000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.374247545.0000000000F2F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.374247545.0000000000F2F000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.374247545.0000000000F2F000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.374514988.0000000000F00000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.374514988.0000000000F00000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.374514988.0000000000F00000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.374514988.0000000000F00000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.373739340.0000000000EC7000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.373739340.0000000000EC7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.373739340.0000000000EC7000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.373739340.0000000000EC7000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.375042801.0000000000E92000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.375042801.0000000000E92000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.375042801.0000000000E92000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.375042801.0000000000E92000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: RegSvcs.exe PID: **2756**, Parent PID: **2200**

General

Target ID:	22
Start time:	17:52:18
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x350000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.376441556.0000000003BE9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.376441556.0000000003BE9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000016.00000002.376441556.0000000003BE9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.375961002.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.375961002.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000016.00000002.375961002.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.374007081.0000000000722000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.374007081.0000000000722000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.374007081.0000000000722000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000016.00000002.374007081.0000000000722000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **2344**, Parent PID: **3320**

General

Target ID:	23
Start time:	17:52:23
Start date:	03/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xb80000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **3696**, Parent PID: **2344**

General

Target ID:	24
Start time:	17:52:23
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **2884**, Parent PID: **5948**

General

Target ID:	25
Start time:	17:52:28
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xa50000

File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: ihgsvw.exe PID: **5040**, Parent PID: **3320**

General

Target ID:	26
Start time:	17:52:33
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
Imagebase:	0xba0000
File size:	1357068 bytes
MD5 hash:	797174324A2A71F55AD4E89DA918B52D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.407827944.00000000012FC000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.407827944.00000000012FC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.407827944.00000000012FC000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001A.00000003.407827944.00000000012FC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.408428728.0000000001293000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.408428728.0000000001293000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.408428728.0000000001293000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001A.00000003.408428728.0000000001293000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.408249022.0000000001300000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.408249022.0000000001300000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.408249022.0000000001300000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001A.00000003.408249022.0000000001300000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.408583600.0000000003BA3000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.408583600.0000000003BA3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.408583600.0000000003BA3000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001A.00000003.408583600.0000000003BA3000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000003.408839619.00000000012C7000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000003.408839619.00000000012C7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000003.408839619.00000000012C7000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001A.00000003.408839619.00000000012C7000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: wscript.exe PID: **3384**, Parent PID: **3320**

General

Target ID:	27
Start time:	17:52:41
Start date:	03/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false

Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs"
Imagebase:	0x7ff6f21c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **1724**, Parent PID: **5040**

General	
Target ID:	28
Start time:	17:52:44
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x950000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: ihgsvw.exe PID: **2788**, Parent PID: **3384**

General	
Target ID:	29
Start time:	17:52:44
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
Imagebase:	0xba0000
File size:	1357068 bytes
MD5 hash:	797174324A2A71F55AD4E89DA918B52D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.431923501.0000000003C1A000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.431923501.0000000003C1A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.431923501.0000000003C1A000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.431923501.0000000003C1A000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.431564388.00000000012A2000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.431564388.00000000012A2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.431564388.00000000012A2000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.431564388.00000000012A2000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.430480318.00000000012D6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.430480318.00000000012D6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.430480318.00000000012D6000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.430480318.00000000012D6000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.430608111.000000000130B000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.430608111.000000000130B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.430608111.000000000130B000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.430608111.000000000130B000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.432175450.00000000012D5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.432175450.00000000012D5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.432175450.00000000012D5000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.432175450.00000000012D5000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.431239930.000000000132B000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.431239930.000000000132B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.431239930.000000000132B000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.431239930.000000000132B000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.430740099.000000000133E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.430740099.000000000133E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.430740099.000000000133E000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.430740099.000000000133E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000003.431128106.000000000130F000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000003.431128106.000000000130F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000003.431128106.000000000130F000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001D.00000003.431128106.000000000130F000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: RegSvcs.exe PID: **5632**, Parent PID: **2788**

General

Target ID:	32
Start time:	17:52:55
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xf30000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET

Analysis Process: ihgsvw.exe PID: **5648**, Parent PID: **3320**

General

Target ID:	33
Start time:	17:52:56
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
Imagebase:	0xba0000
File size:	1357068 bytes
MD5 hash:	797174324A2A71F55AD4E89DA918B52D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000021.00000003.467106466.0000000000F6E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000003.467106466.0000000000F6E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000003.467106466.0000000000F6E000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000021.00000003.467106466.0000000000F6E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000021.00000003.467835981.0000000000F05000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000003.467835981.0000000000F05000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000003.467835981.0000000000F05000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000021.00000003.467835981.0000000000F05000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000021.00000003.468424506.0000000000F38000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000003.468424506.0000000000F38000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000003.468424506.0000000000F38000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000021.00000003.468424506.0000000000F38000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000021.00000003.467996815.00000000039C0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000003.467996815.00000000039C0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000003.467996815.00000000039C0000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000021.00000003.467996815.00000000039C0000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000021.00000003.467618128.0000000000F72000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000003.467618128.0000000000F72000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000003.467618128.0000000000F72000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000021.00000003.467618128.0000000000F72000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: wscript.exe PID: **5884**, Parent PID: **3320**

General

Target ID:	34
Start time:	17:53:05
Start date:	03/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user~1\AppData\Local\Temp\FOLDER~1\Update.vbs"
Imagebase:	0x7ff6f21c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ihgsvw.exe PID: **5304**, Parent PID: **5884**

General	
Target ID:	35
Start time:	17:53:06
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder10_51\ihgsvw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\FOLDER~1\ihgsvw.exe" C:\Users\user~1\AppData\Local\Temp\FOLDER~1\CCMBPO~1.DOC
Imagebase:	0xba0000
File size:	1357068 bytes
MD5 hash:	797174324A2A71F55AD4E89DA918B52D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.486991212.00000000017DF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.486991212.00000000017DF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.486991212.00000000017DF000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.486991212.00000000017DF000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.487823598.00000000042C1000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.487823598.00000000042C1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.487823598.00000000042C1000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.487823598.00000000042C1000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.482858075.0000000001810000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.482858075.0000000001810000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.482858075.0000000001810000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.482858075.0000000001810000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.487203996.00000000017FB000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.487203996.00000000017FB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.487203996.00000000017FB000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.487203996.00000000017FB000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.487454794.0000000001773000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.487454794.0000000001773000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.487454794.0000000001773000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.487454794.0000000001773000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.488033967.00000000017A7000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.488033967.00000000017A7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.488033967.00000000017A7000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.488033967.00000000017A7000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.481255588.00000000017DC000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.481255588.00000000017DC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.481255588.00000000017DC000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.481255588.00000000017DC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000003.481046485.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000003.481046485.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000003.481046485.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000023.00000003.481046485.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: RegSvcs.exe PID: **4588**, Parent PID: **5648**

General

Target ID:	36
Start time:	17:53:12
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x7b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: RegSvcs.exe PID: **4768**, Parent PID: **5304**

General	
Target ID:	37
Start time:	17:53:20
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xa0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly