ID: 355626
Sample Name: CHEQUE COPY.exe
Cookbook: default.jbs
Time: 09:28:14
Date: 20/02/2021
Version: 31.0.0 Emerald

Table of Contents

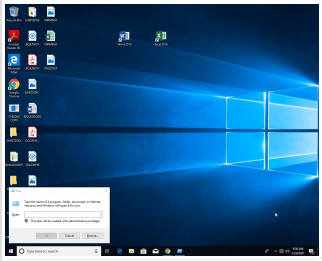
Analysis Report CHEQUE COPY.exe

Overview

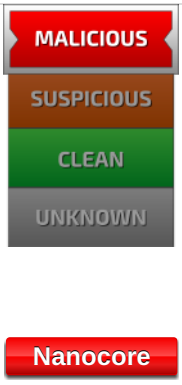
General Information

Sample Name:	CHEQUE COPY.exe
Analysis ID:	355626
MD5:	ec067b73f3156ae.
SHA1:	6353de54ce12dfd.
SHA256:	3f6f1635ca9660f…
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



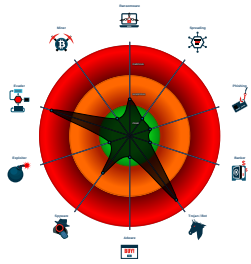
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- CHEQUE COPY.exe (PID: 6828 cmdline: 'C:\Users\user\Desktop\CHEQUE COPY.exe' MD5: EC067B73F3156AEDBD9158F107952EB8)
  - CHEQUE COPY.exe (PID: 6924 cmdline: 'C:\Users\user\Desktop\CHEQUE COPY.exe' MD5: EC067B73F3156AEDBD9158F107952EB8)
    - schtasks.exe (PID: 7096 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 7148 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp811A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- CHEQUE COPY.exe (PID: 6200 cmdline: 'C:\Users\user\Desktop\CHEQUE COPY.exe' 0 MD5: EC067B73F3156AEDBD9158F107952EB8)
  - CHEQUE COPY.exe (PID: 5852 cmdline: 'C:\Users\user\Desktop\CHEQUE COPY.exe' 0 MD5: EC067B73F3156AEDBD9158F107952EB8)
- dhcpmon.exe (PID: 6116 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: EC067B73F3156AEDBD9158F107952EB8)
  - dhcpmon.exe (PID: 6356 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: EC067B73F3156AEDBD9158F107952EB8)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "bed38ea9-13ae-4999-bfd6-9ec5f9de3405",
  "Group": "Default",
  "Domain1": "chinomso.duckdns.org",
  "Domain2": "chinomso.duckdns.org",
  "Port": 7688,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "chinomso.duckdns.org",
  "BackupDNSServer": "chinomso.duckdns.orgAMC9Avo9uFWUE1JbxpU=",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.688775764.00000000026C0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1c85b:$a: NanoCore • 0x1c8b4:$a: NanoCore • 0x1c8f1:$a: NanoCore • 0x1c96a:$a: NanoCore • 0x1c8bd:$b: ClientPlugin • 0x1c8fa:$b: ClientPlugin • 0x1d1f8:$b: ClientPlugin • 0x1d205:$b: ClientPlugin • 0x129df:$e: KeepAlive • 0x1cd45:$g: LogClientMessage • 0x1ccc5:$i: get_Connected • 0xcc91:$j: #=q • 0xccc1:$j: #=q • 0xccfd:$j: #=q • 0xcd25:$j: #=q • 0xcd55:$j: #=q • 0xcd85:$j: #=q • 0xcdb5:$j: #=q • 0xcde5:$j: #=q • 0xce01:$j: #=q • 0xce31:$j: #=q
0000000B.00000002.672768392.000000000347C000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.672768392.000000000347C000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x43195:$a: NanoCore • 0x431ee:$a: NanoCore • 0x4322b:$a: NanoCore • 0x432a4:$a: NanoCore • 0x5694f:$a: NanoCore • 0x56964:$a: NanoCore • 0x56999:$a: NanoCore • 0x6f95b:$a: NanoCore • 0x6f970:$a: NanoCore • 0x6f9a5:$a: NanoCore • 0x431f7:$b: ClientPlugin • 0x43234:$b: ClientPlugin • 0x43b32:$b: ClientPlugin • 0x43b3f:$b: ClientPlugin • 0x5670b:$b: ClientPlugin • 0x56726:$b: ClientPlugin • 0x56756:$b: ClientPlugin • 0x5696d:$b: ClientPlugin • 0x569a2:$b: ClientPlugin • 0x6f717:$b: ClientPlugin • 0x6f732:$b: ClientPlugin
0000000F.00000002.688804869.000000000367000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x146bd:$x1: NanoCore.ClientPluginHost • 0x146fa:$x2: IClientNetworkHost • 0x1822d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000002.688804869.000000000367000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 109 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.CHEQUE COPY.exe.2dc1458.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
10.2.CHEQUE COPY.exe.2dc1458.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
10.2.CHEQUE COPY.exe.2dc1458.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
10.2.CHEQUE COPY.exe.2dc1458.4.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:$j: #=q
11.2.CHEQUE COPY.exe.415058.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 303 entries				

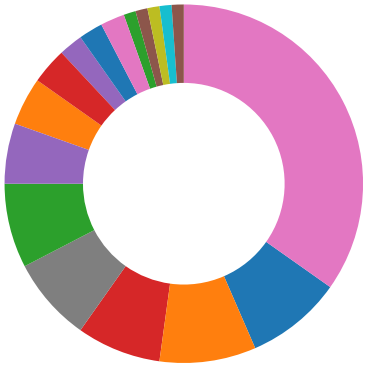
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

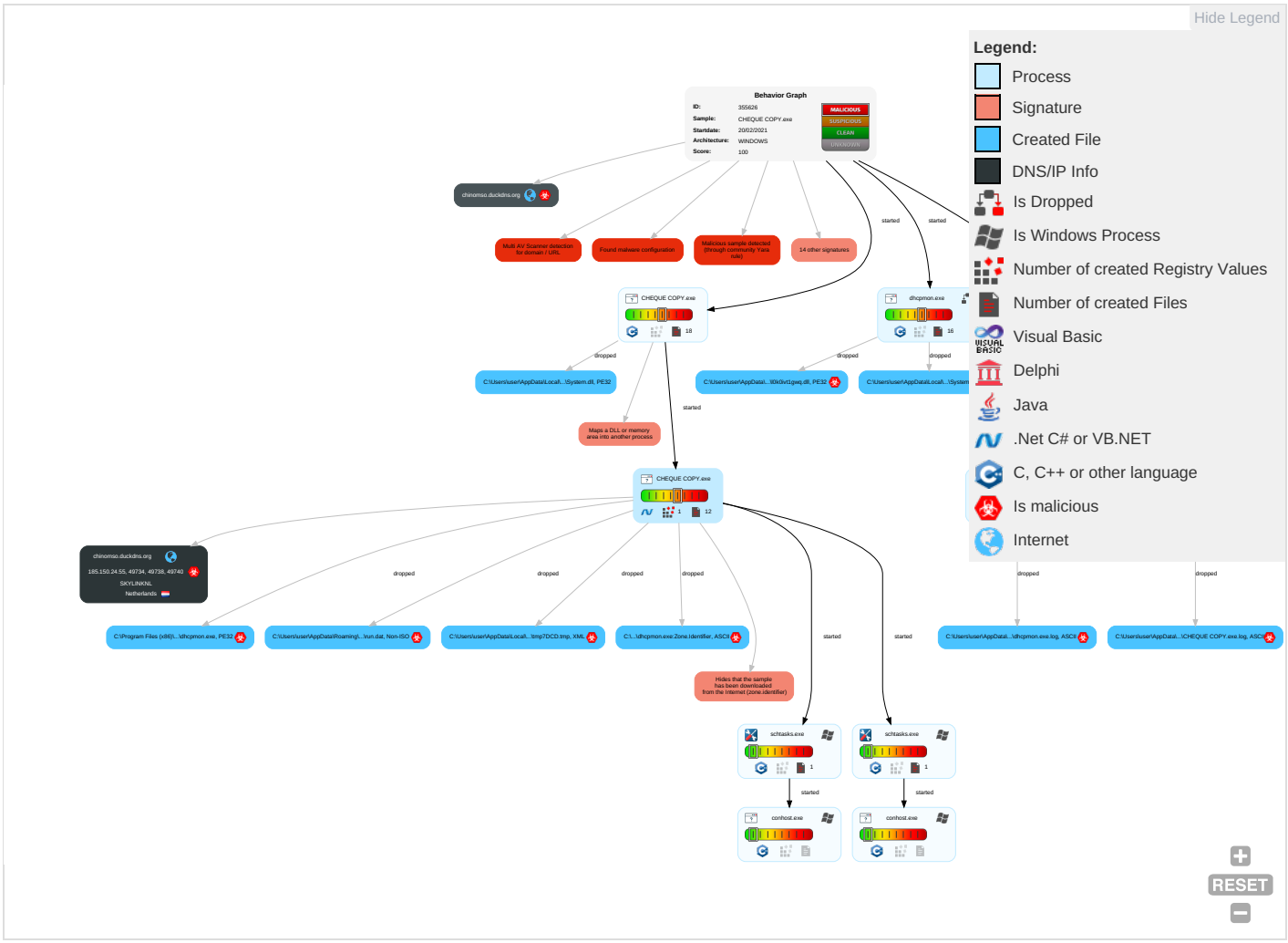
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 2 5	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 2	NTDS	Security Software Discovery 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

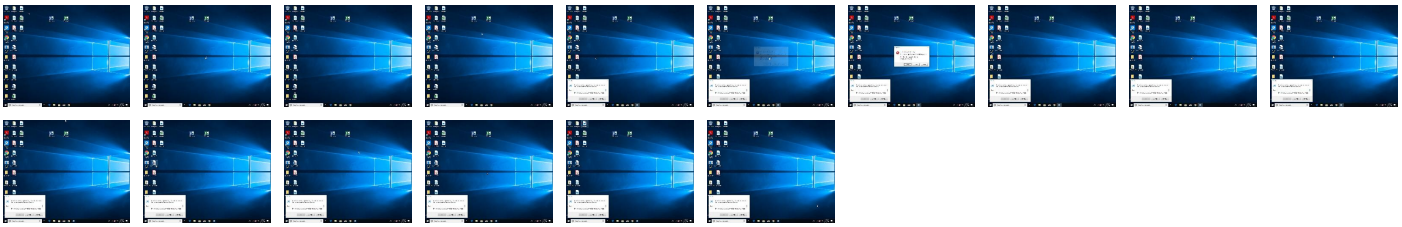
Behavior Graph



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
CHEQUE COPY.exe	45%	Virustotal		Browse
CHEQUE COPY.exe	28%	ReversingLabs	Win32.Backdoor.NanoBot	
CHEQUE COPY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	45%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	28%	ReversingLabs	Win32.Backdoor.NanoBot	
C:\Users\user\AppData\Local\Temp\l0k0ivt1gwq.dll	17%	ReversingLabs	Win32.Trojan.Cerbu	
C:\Users\user\AppData\Local\Temp\nsj85AE.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsj85AE.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsx694C.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsx694C.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.1.CHEQUE COPY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.1.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.CHEQUE COPY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.CHEQUE COPY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.CHEQUE COPY.exe.4a60000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.1.CHEQUE COPY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.CHEQUE COPY.exe.4fc0000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.dhcpmon.exe.4a60000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.CHEQUE COPY.exe.58c0000.13.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
chinomso.duckdns.org	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
chinomso.duckdns.org	8%	Virustotal		Browse
chinomso.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chinomso.duckdns.org	185.150.24.55	true	true	• 8%, Virustotal, Browse	unknown

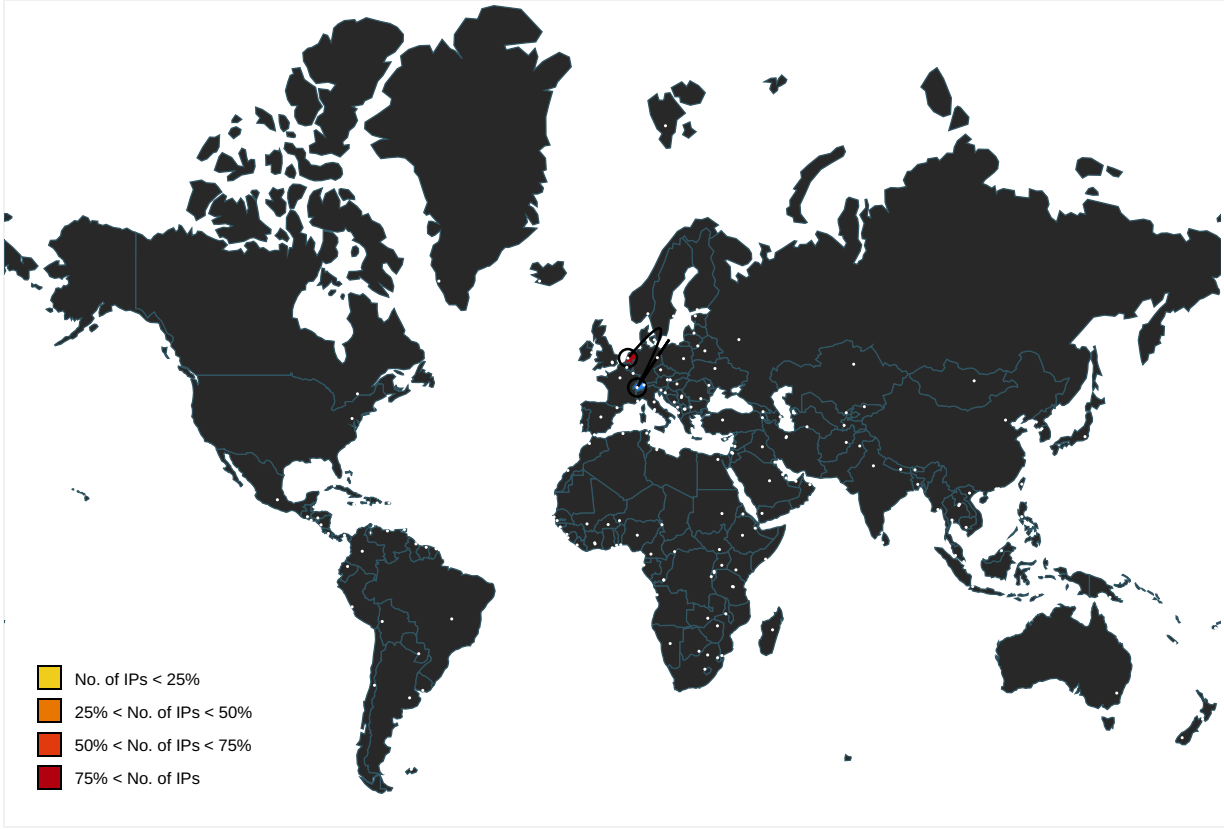
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
chinomso.duckdns.org	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	CHEQUE COPY.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	CHEQUE COPY.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.150.24.55	unknown	Netherlands		44592	SKYLINKNL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355626
Start date:	20.02.2021
Start time:	09:28:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CHEQUE COPY.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/17@23/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 11.5% (good quality ratio 10.7%) • Quality average: 78.2% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 92.122.145.220, 104.43.139.144, 13.88.21.125, 52.255.188.83, 51.104.146.109, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 51.104.139.180, 92.122.213.247, 92.122.213.194, 51.132.208.181 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
09:29:03	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\CHEQUE COPY.exe" s>$(Arg0)
09:29:03	API Interceptor	1031x Sleep call for process: CHEQUE COPY.exe modified
09:29:03	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:29:05	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.150.24.55	CHEQUE COPY.jar	Get hash	malicious	Browse	
	PAYMENT COPY RECEIPT.exe	Get hash	malicious	Browse	
	FeDEx TRACKING DETAILS.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FeDEx TRACKING DETAILS.exe	Get hash	malicious	Browse	
	FedEx TRACKING DETAILS.exe	Get hash	malicious	Browse	
	TNT TRACKING DETAILS.exe	Get hash	malicious	Browse	
	TNT TRACKING DETAILS.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
chinomso.duckdns.org	PAYMENT COPY RECEIPT.exe	Get hash	malicious	Browse	• 185.150.24.55
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	DHL AWB TRACKING DETAIL.exe	Get hash	malicious	Browse	• 194.5.98.56
	odou7cg844.exe	Get hash	malicious	Browse	• 129.205.124.145
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.244.30.86
	AWB RECEIPT.exe	Get hash	malicious	Browse	• 129.205.124.132
	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 129.205.113.246
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 197.210.227.36
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.244.30.39
	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 129.205.124.140
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 197.210.85.85
	DHL AWB TRACKING DETAIILS.exe	Get hash	malicious	Browse	• 185.244.30.39
	39Quot.exe	Get hash	malicious	Browse	• 185.165.153.35

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SKYLINKNL	Quotation-3276.PDF.exe	Get hash	malicious	Browse	• 185.150.24.44
	CHEQUE COPY.jar	Get hash	malicious	Browse	• 185.150.24.55
	MRC20201030XMY, pdf.exe	Get hash	malicious	Browse	• 185.150.24.6
	PAYMENT COPY RECEIPT.exe	Get hash	malicious	Browse	• 185.150.24.55
	FeDEx TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.150.24.55
	FeDEx TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.150.24.55
	FedEx TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.150.24.55
	TNT TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.150.24.55
	TNT TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.150.24.55
	QUOTATION 20 10 2020.exe	Get hash	malicious	Browse	• 185.150.24.48
	NEW PO638363483.exe	Get hash	malicious	Browse	• 185.150.24.9
	NEW PO6487382.exe	Get hash	malicious	Browse	• 185.150.24.9

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsj85AE.tmp\System.dll	Bank Details.exe	Get hash	malicious	Browse	
	Re-QUOTATION.exe	Get hash	malicious	Browse	
	shed.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	QUOTATION_PDF_SCAN_COPY.exe	Get hash	malicious	Browse	
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	
	Firm Order.exe	Get hash	malicious	Browse	
	Documents_pdf.exe	Get hash	malicious	Browse	
	QUOTATION.exe	Get hash	malicious	Browse	
	banka bilgisi.exe	Get hash	malicious	Browse	
	MV TEAL BULKERS.xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	
	HBL VRNA00872.xlsx	Get hash	malicious	Browse	
	statement.xlsx	Get hash	malicious	Browse	
	_Doc_Shipment_330393_.xlsx	Get hash	malicious	Browse	
	HBL VRN0924588.xlsx	Get hash	malicious	Browse	
	SHED.EXE	Get hash	malicious	Browse	
	c4p1vG05Z8.exe	Get hash	malicious	Browse	
	Offer18022021.xlsx	Get hash	malicious	Browse	
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp\System.dll	Bank Details.exe	Get hash	malicious	Browse	
	Re-QUOTATION.exe	Get hash	malicious	Browse	
	shed.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	QUOTATION_PDF_SCAN_COPY.exe	Get hash	malicious	Browse	
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	
	Firm Order.exe	Get hash	malicious	Browse	
	Documents_pdf.exe	Get hash	malicious	Browse	
	QUOTATION.exe	Get hash	malicious	Browse	
	banka bilgisi.exe	Get hash	malicious	Browse	
	MV TEAL BULKERS.xlsx	Get hash	malicious	Browse	
	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	
	HBL VRNA00872.xlsx	Get hash	malicious	Browse	
	statement.xlsx	Get hash	malicious	Browse	
	_Doc_Shipment_330393_.xlsx	Get hash	malicious	Browse	
	HBL VRN0924588.xlsx	Get hash	malicious	Browse	
	SHED.EXE	Get hash	malicious	Browse	
	c4p1vG05Z8.exe	Get hash	malicious	Browse	
	Offer18022021.xlsx	Get hash	malicious	Browse	
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	331665
Entropy (8bit):	7.943201162388639
Encrypted:	false
SSDEEP:	6144:Lx/MKNJ1v1P/51wTavAPyVCow2do2dZo8bBU2lVWoZmriV:B5T1tPxSPyVDdLP9VBkq
MD5:	EC067B73F3156AEDBD9158F107952EB8
SHA1:	6353DE54CE12DFD2CD86A3DC2824C7448157A821
SHA-256:	3F6F1635CA9660F24BF4E9527EC6136ED50AD9A8A88E442768143D55EB73A6AF
SHA-512:	83456705E8BED761FC5091CDE0395314968327FD4929CBC79BD4350765328DF66FE2EE00D9D66A0B23B1246FE44B19C6F3CB3CD3BBBA88E0827442C5E8B7958
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 45%, Browse • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!.@.@...@...@../O...@...@..L@../O...@...c...@..+F...@..Rich.@ .....PE..L...%.$_.....d....9.....%3.....@.....:.....@.....8.....:.|..... .....text...0b.....d..... ..`.rdata..t.....h.....@..@.data...x.9.....|.....@....ndata.....@:.....rsrc...|.....:.....@..@..... ....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CHEQUE COPY.exe.log	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\l0k0ivt1gwq.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	6.946221991408385
Encrypted:	false
SSDEEP:	192:MeNibu5S6oJROvgAPu8vf1L0HZtbuxw9HqjZ7:E60avgAP3fVSbf5qj
MD5:	8FEC1FE4587680848AB0D0B5F0FD7D62
SHA1:	7192AF111E78841F12772D3C82E2BE33EFAAA28D
SHA-256:	553656F7C7BCCCF8EFF0A2F92D843C194404E5E1A743ABC50C3904A1781168FA

C:\Users\user\AppData\Local\Temp\l0k0ivt1gwq.dll	
SHA-512:	254390CDD8565E4A2EF92F3C450228BC470EC09F94D6AABDAAA7115EEC5F2C0601F9BA88278B70C4595766A7C42A05BE903FCC63444A0E1A119764AB86887BC8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&8u.bY..bY..bY..bY..tY.....oY..E..cY..E..cY..E..cY..RichbY..... .....PE..L....l0`.....!..... ..... .....P.....@#..H...p ..... ..p..... .....text..... ..`.rdata..... .....@..@.data.....0.....@..... ....

C:\Users\user\AppData\Local\Temp\mkecgmj.p	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	279040
Entropy (8bit):	**7.999364271075393**
Encrypted:	**true**
SSDEEP:	6144:P1v1P/51wTavAPyVCow2do2dZo8bBU2lVWoZmrii:P1tPxSPyVDdLP9VBkr
MD5:	38FCBFD0FE1E67D1B13FF1A60CA4E8E2
SHA1:	55ED4A22CB76D20406B1FB042415D89697223A6C
SHA-256:	52B03BF52B4638A5AECB44A436B01A612FB261920FAE67A5DAC0E54CD9EDD574
SHA-512:	47B174E568A37F91B49396F5FC7B1B348BF91A2E6B0B06D14CFA0321CAB0BFF0C151FBE00B9B9B2E810525D8A4627AE376268766A54E792D1229E7607476F51A
Malicious:	false
Reputation:	low
Preview:	p.L.."SL<. 4.....`...e\.'.S...T.4~..w.%K.m.....p.P.....l;.r.n..~..Z.3).....R...#.J."YY...V..'../..U^u..B.?f*,Y.....2.....OeB.k,..,m..]l..*.....{}J.Y5....o..%g...}.a&.....s0..+..=.>^.... @.}..@..9.T.9.gD\..=:.4.a..*Q2...l.e.|..f{.X..R.C,.l.f+....V.|.. .E..sN....W..hu{<. W..U..E.....a.F.Lc.F.....S..E.....T.....,t.b.T...7h...1...)....[[j`..#.+.U."%K..+.....D\=..JB.-g.....d.c. Q.c6....3....D.C..gQ..y.PK ....<G...w....r..!.H...0.$.#....Y.H.d.S..C...o..Y.....3.M_....d.l.}){...r.4.....ZI.]5.. ].D%~M.4.{.B....L.l..}.....x....O.0..g....P.t+.*.G.j.`.x]\e.....@DZb ..Q.S.*.|....;..v.;r.|.T.R.[E.@e@....5.,.v.\q...uz*.a.+"....O...N.%<,...w.j..k...~...UM..o.j..+.,N.~..UM....u...).d.....R.....".j.L f.,.j....'..aE.....Q..'i.....-cJ9..u.r.$.nLXi....Sx.i{.....n.. =..../.$..+.C.^>...V..N\.n.(*m...Q....i%..P.Q..3 ..e>.)"u.GH!".a..c~f.SJ.8b...k.B.5.,0.....@...M..=.}.l.(.2....X.....jwL.....#.z...1.h$....RF....".....5..8.....

C:\Users\user\AppData\Local\Temp\nsj85AE.tmp\System.dll	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Bank Details.exe, Detection: malicious, Browse • Filename: Re-QUOTATION.exe, Detection: malicious, Browse • Filename: shed.exe, Detection: malicious, Browse • Filename: purchase order.exe, Detection: malicious, Browse • Filename: QUOTATION_PDF_SCAN_COPY.exe, Detection: malicious, Browse • Filename: DHL Shipment Notification 7465649870,pdf.exe, Detection: malicious, Browse • Filename: Firm Order.exe, Detection: malicious, Browse • Filename: Documents_pdf.exe, Detection: malicious, Browse • Filename: QUOTATION.exe, Detection: malicious, Browse • Filename: banka bilgisi.exe, Detection: malicious, Browse • Filename: MV TEAL BULKERS.xlsx, Detection: malicious, Browse • Filename: ForeignRemittance_20210219_USD.xlsx, Detection: malicious, Browse • Filename: HBL VRNA00872.xlsx, Detection: malicious, Browse • Filename: statement.xlsx, Detection: malicious, Browse • Filename: _Doc_Shipment_330393_.xlsx, Detection: malicious, Browse • Filename: HBL VRN0924588.xlsx, Detection: malicious, Browse • Filename: SHED.EXE, Detection: malicious, Browse • Filename: c4p1vG05Z8.exe, Detection: malicious, Browse • Filename: Offer18022021.xlsx, Detection: malicious, Browse • Filename: DHL Shipment Notification 7465649870.pdf.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\nsj85AE.tmp\System.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp\System.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Bank Details.exe, Detection: malicious, Browse • Filename: Re-QUOTATION.exe, Detection: malicious, Browse • Filename: shed.exe, Detection: malicious, Browse • Filename: purchase order.exe, Detection: malicious, Browse • Filename: QUOTATION_PDF_SCAN_COPY.exe, Detection: malicious, Browse • Filename: DHL Shipment Notification 7465649870,pdf.exe, Detection: malicious, Browse • Filename: Firm Order.exe, Detection: malicious, Browse • Filename: Documents_pdf.exe, Detection: malicious, Browse • Filename: QUOTATION.exe, Detection: malicious, Browse • Filename: banka bilgisi.exe, Detection: malicious, Browse • Filename: MV TEAL BULKERS.xlsx, Detection: malicious, Browse • Filename: ForeignRemittance_20210219_USD.xlsx, Detection: malicious, Browse • Filename: HBL VRNA00872.xlsx, Detection: malicious, Browse • Filename: statement.xlsx, Detection: malicious, Browse • Filename: _Doc_Shipment_330393_.xlsx, Detection: malicious, Browse • Filename: HBL VRN0924588.xlsx, Detection: malicious, Browse • Filename: SHED.EXE, Detection: malicious, Browse • Filename: c4p1vG05Z8.exe, Detection: malicious, Browse • Filename: Offer18022021.xlsx, Detection: malicious, Browse • Filename: DHL Shipment Notification 7465649870.pdf.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsx694C.tmp\System.dll	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp	
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.115251788848742
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Yq8xtn:cbk4oL600QydbQxIYODOLedq3+8j
MD5:	121D7A1A91E22CE2154D0260A83DE375
SHA1:	E1A642F6194608F5A0D896739A75EE2A07E9E4FC
SHA-256:	5B036902A33AA54797EB0118780D6226372231AF995C260FD163324DF788623C
SHA-512:	642829EBCC236DE0023BF62FFC66294478CC9CE439622464BFF2D72FE1F5E07A8EA1C93177F5CD3D6354CE3E94B974821D5594FED267070483A4AB21A15B337
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp811A.tmp	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.5
Encrypted:	false
SSDEEP:	3:Dn:D
MD5:	BD1968E6793B05071285CEC4355C6C8E
SHA1:	091BC05662A578369E91AF9A1AC0436C3432F3CC
SHA-256:	4F57377900A157775B7D1644D33219445FAA0EEA90EDF2C1D1984001EF4A6A74
SHA-512:	E9A999866CE5628D266CA4A1DA0577389369BE95F49ED9D2030A0DA0B812B18F5F57632436E8DDB62730B5E0027528FFB50494208CA01F858E5F79153E948C56
Malicious:	**true**
Preview:	y..y..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\CHEQUE COPY.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.238334671954105
Encrypted:	false
SSDEEP:	3:oNt+WfWmS0+q20dA:oNwvmH+TkA
MD5:	3FC5217BE7ACC87B0E5B62A0D947C252
SHA1:	75211E26E82408BE79D04E78CB04E9ECAA18EC0F
SHA-256:	8BA635B37D08E3DAC020EC35190334F6F8A650084AD6A51493133DEBCCF27E1A

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SHA-512:	05DAB8B2D1E3A2DABA4A583B367A51A9F295109296E9F3B74ECBAA761D0F92372FB53A1A7ECF6F112B5D87F41804591F03849BC384DD494BF2B7E6EC3DAAF0E8
Malicious:	false
Preview:	C:\Users\user\Desktop\CHEQUE COPY.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.943201162388639
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:	CHEQUE COPY.exe
File size:	331665
MD5:	ec067b73f3156aedbd9158f107952eb8
SHA1:	6353de54ce12dfd2cd86a3dc2824c7448157a821
SHA256:	3f6f1635ca9660f24bf4e9527ec6136ed50ad9a8a88e442768143d55eb73a6af
SHA512:	83456705e8bed761fc5091cde0395314968327fd4929cbc79bd4350765328df66fe2ee00d9d66a0b23b1246fe44b19c6f3cb3cd3bbba88e0827442c5e8b79585
SSDEEP:	6144:Lx/MKNJ1v1P/51wTavAPyVCow2do2dZo8bBU2lVWoZmriV:B5T1tPxSPyVDdLP9VBkq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!.@.@.....@...@../O...@...@..L@../O...@...c...@..+F...@..Rich.@.....PE..L...%.$_.....d....9....%3.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403325
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D625 [Sat Aug 1 02:40:37 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A2F6Ch], eax
je 00007FF5948A80D3h
push ebx
call 00007FF5948AB236h
cmp eax, ebx
je 00007FF5948A80C9h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007FF5948AB1B2h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FF5948A80ADh
push 0000000Bh
call 00007FF5948AB20Ah
push 00000009h
call 00007FF5948AB203h
push 00000007h
mov dword ptr [007A2F64h], eax
call 00007FF5948AB1F7h
cmp eax, ebx
je 00007FF5948A80D1h
push 0000001Eh
call eax
test eax, eax
je 00007FF5948A80C9h
or byte ptr [007A2F6Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [007A3038h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0079E528h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x97c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0x6230	0x6400	False	0.6699609375	data	6.44188995255	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.4337890625	data	5.06106734837	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x399078	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x97c	0xa00	False	0.455078125	data	4.30771149045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x3ac148	0x100	data	English	United States
RT_DIALOG	0x3ac248	0x11c	data	English	United States
RT_DIALOG	0x3ac364	0x60	data	English	United States
RT_VERSION	0x3ac3c4	0x278	data	English	United States
RT_MANIFEST	0x3ac63c	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Version Infos

Description	Data
LegalCopyright	Copyright orientation
FileVersion	68.67.88.38
CompanyName	fire escape
LegalTrademarks	Ap Ma
Comments	shoreline
ProductName	gaoler
FileDescription	Barton's echidna
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 110

- 53 (DNS)
- 7688 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 09:29:04.682451010 CET	49734	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:04.737190962 CET	7688	49734	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:05.244375944 CET	49734	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:05.298325062 CET	7688	49734	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:05.806895971 CET	49734	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:05.861803055 CET	7688	49734	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:10.216090918 CET	49738	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:10.269927979 CET	7688	49738	185.150.24.55	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 09:29:10.770991087 CET	49738	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:10.827547073 CET	7688	49738	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:11.333467007 CET	49738	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:11.387327909 CET	7688	49738	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:15.874444962 CET	49740	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:15.929754019 CET	7688	49740	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:16.443367004 CET	49740	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:16.500091076 CET	7688	49740	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:17.006696939 CET	49740	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:17.060661077 CET	7688	49740	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:21.173434019 CET	49743	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:21.228018999 CET	7688	49743	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:21.740602016 CET	49743	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:21.794497967 CET	7688	49743	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:22.303168058 CET	49743	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:22.357170105 CET	7688	49743	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:26.479995012 CET	49744	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:26.533838034 CET	7688	49744	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:27.038095951 CET	49744	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:27.091991901 CET	7688	49744	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:27.600374937 CET	49744	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:27.655774117 CET	7688	49744	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:31.763168097 CET	49745	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:31.817127943 CET	7688	49745	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:32.319502115 CET	49745	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:32.373542070 CET	7688	49745	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:32.882119894 CET	49745	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:32.936161041 CET	7688	49745	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:37.042965889 CET	49746	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:37.096920013 CET	7688	49746	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:37.601248980 CET	49746	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:37.659624100 CET	7688	49746	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:38.226260900 CET	49746	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:38.280384064 CET	7688	49746	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:42.573045015 CET	49755	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:42.626921892 CET	7688	49755	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:43.132951021 CET	49755	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:43.188443899 CET	7688	49755	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:43.695447922 CET	49755	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:43.752320051 CET	7688	49755	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:48.163765907 CET	49760	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:48.219160080 CET	7688	49760	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:48.727157116 CET	49760	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:48.783839941 CET	7688	49760	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:49.289788961 CET	49760	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:49.343722105 CET	7688	49760	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:53.434062958 CET	49761	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:53.487981081 CET	7688	49761	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:53.993300915 CET	49761	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:54.047264099 CET	7688	49761	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:54.555854082 CET	49761	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:54.609582901 CET	7688	49761	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:58.803488016 CET	49765	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:58.857521057 CET	7688	49765	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:59.368655920 CET	49765	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:59.423696995 CET	7688	49765	185.150.24.55	192.168.2.4
Feb 20, 2021 09:29:59.931174994 CET	49765	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:29:59.985225916 CET	7688	49765	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:04.309041023 CET	49771	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:04.362966061 CET	7688	49771	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:04.884762049 CET	49771	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:04.938821077 CET	7688	49771	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:05.447323084 CET	49771	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:05.502799034 CET	7688	49771	185.150.24.55	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 09:30:10.047544956 CET	49772	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:10.101521969 CET	7688	49772	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:10.603966951 CET	49772	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:10.659145117 CET	7688	49772	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:11.166527033 CET	49772	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:11.220618963 CET	7688	49772	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:15.506270885 CET	49773	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:15.564398050 CET	7688	49773	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:16.073276043 CET	49773	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:16.127351046 CET	7688	49773	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:16.635855913 CET	49773	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:16.692507029 CET	7688	49773	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:20.855978012 CET	49774	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:20.910017014 CET	7688	49774	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:21.417545080 CET	49774	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:21.474658966 CET	7688	49774	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:21.979948044 CET	49774	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:22.034101963 CET	7688	49774	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:26.128468990 CET	49775	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:26.182354927 CET	7688	49775	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:26.683466911 CET	49775	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:26.740122080 CET	7688	49775	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:27.246012926 CET	49775	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:27.302422047 CET	7688	49775	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:31.390067101 CET	49776	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:31.444163084 CET	7688	49776	185.150.24.55	192.168.2.4
Feb 20, 2021 09:30:31.949481964 CET	49776	7688	192.168.2.4	185.150.24.55
Feb 20, 2021 09:30:32.005574942 CET	7688	49776	185.150.24.55	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 09:28:50.858154058 CET	59123	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:50.908090115 CET	53	59123	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:51.822695971 CET	54531	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:51.874311924 CET	53	54531	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:51.942909956 CET	49714	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:52.004360914 CET	53	49714	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:52.760857105 CET	58028	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:52.818367958 CET	53	58028	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:53.703960896 CET	53097	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:53.764658928 CET	53	53097	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:54.935142994 CET	49257	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:54.984257936 CET	53	49257	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:55.869863033 CET	62389	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:55.921323061 CET	53	62389	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:56.836747885 CET	49910	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:56.885438919 CET	53	49910	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:57.818181038 CET	55854	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:57.869813919 CET	53	55854	8.8.8.8	192.168.2.4
Feb 20, 2021 09:28:58.820045948 CET	64549	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:28:58.881336927 CET	53	64549	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:00.259080887 CET	63153	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:00.308000088 CET	53	63153	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:01.280355930 CET	52991	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:01.338788033 CET	53	52991	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:02.409961939 CET	53700	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:02.469748974 CET	53	53700	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:03.362679958 CET	51726	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:03.415625095 CET	53	51726	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:04.409420967 CET	56794	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:04.445300102 CET	56534	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:04.458153963 CET	53	56794	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:04.665582895 CET	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 09:29:07.798640013 CET	56627	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:07.850261927 CET	53	56627	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:08.764969110 CET	56621	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:08.813744068 CET	53	56621	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:09.732856035 CET	63116	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:09.783145905 CET	53	63116	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:09.988846064 CET	64078	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:10.213303089 CET	53	64078	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:10.681179047 CET	64801	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:10.729827881 CET	53	64801	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:15.561894894 CET	61721	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:15.782841921 CET	53	61721	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:20.484283924 CET	51255	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:20.535968065 CET	53	51255	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:21.097795963 CET	61522	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:21.157784939 CET	53	61522	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:26.427056074 CET	52337	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:26.478487015 CET	53	52337	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:31.700709105 CET	55046	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:31.760209084 CET	53	55046	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:36.980783939 CET	49612	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:37.038008928 CET	53	49612	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:38.048086882 CET	49285	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:38.125420094 CET	53	49285	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:38.646158934 CET	50601	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:38.726509094 CET	53	50601	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:39.269819975 CET	60875	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:39.341459036 CET	53	60875	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:39.462989092 CET	56448	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:39.566857100 CET	53	56448	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:39.999485970 CET	59172	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:40.056739092 CET	53	59172	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:40.618684053 CET	62420	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:40.679446936 CET	53	62420	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:41.213634968 CET	60579	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:41.275595903 CET	53	60579	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:41.955435991 CET	50183	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:42.019148111 CET	53	50183	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:42.335110903 CET	61531	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:42.571342945 CET	53	61531	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:42.915522099 CET	49228	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:42.972665071 CET	53	49228	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:44.398801088 CET	59794	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:44.456403017 CET	53	59794	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:44.891921043 CET	55916	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:44.948983908 CET	53	55916	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:45.743062019 CET	52752	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:45.806126118 CET	53	52752	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:48.103735924 CET	60542	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:48.162168980 CET	53	60542	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:53.375653028 CET	60689	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:53.433005095 CET	53	60689	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:55.895731926 CET	64206	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:55.947396994 CET	53	64206	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:56.060692072 CET	50904	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:56.120268106 CET	53	50904	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:58.657116890 CET	57525	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:58.705873013 CET	53	57525	8.8.8.8	192.168.2.4
Feb 20, 2021 09:29:58.829284906 CET	53814	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:29:58.901669025 CET	53	53814	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:04.056679964 CET	53418	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:04.296006918 CET	53	53418	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:09.986005068 CET	62833	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:10.046027899 CET	53	62833	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 09:30:15.281327963 CET	59260	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:15.504040956 CET	53	59260	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:20.727509022 CET	49944	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:20.785655022 CET	53	49944	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:26.066606998 CET	63300	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:26.126811981 CET	53	63300	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:31.331859112 CET	61449	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:31.389084101 CET	53	61449	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:31.935074091 CET	51275	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:31.986309052 CET	53	51275	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:33.459094048 CET	63492	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:33.517997980 CET	53	63492	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:36.613883972 CET	58945	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:36.662565947 CET	53	58945	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:41.885508060 CET	60779	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:42.106175900 CET	53	60779	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:47.394042969 CET	64014	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:47.445638895 CET	53	64014	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:52.678965092 CET	57091	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:52.727715015 CET	53	57091	8.8.8.8	192.168.2.4
Feb 20, 2021 09:30:58.011396885 CET	55904	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:30:58.071069002 CET	53	55904	8.8.8.8	192.168.2.4
Feb 20, 2021 09:31:03.359149933 CET	52109	53	192.168.2.4	8.8.8.8
Feb 20, 2021 09:31:03.584403038 CET	53	52109	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 20, 2021 09:29:04.445300102 CET	192.168.2.4	8.8.8.8	0x373a	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:09.988846064 CET	192.168.2.4	8.8.8.8	0xf04d	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:15.561894894 CET	192.168.2.4	8.8.8.8	0x28b9	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:21.097795963 CET	192.168.2.4	8.8.8.8	0x92b2	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:26.427056074 CET	192.168.2.4	8.8.8.8	0x2f7d	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:31.700709105 CET	192.168.2.4	8.8.8.8	0x531a	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:36.980783939 CET	192.168.2.4	8.8.8.8	0x40e0	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:42.335110903 CET	192.168.2.4	8.8.8.8	0x45d	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:48.103735924 CET	192.168.2.4	8.8.8.8	0xe0fb	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:53.375653028 CET	192.168.2.4	8.8.8.8	0x32c9	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:58.657116890 CET	192.168.2.4	8.8.8.8	0x7bd0	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:04.056679964 CET	192.168.2.4	8.8.8.8	0x1d81	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:09.986005068 CET	192.168.2.4	8.8.8.8	0x2336	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:15.281327963 CET	192.168.2.4	8.8.8.8	0x6b7b	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:20.727509022 CET	192.168.2.4	8.8.8.8	0x1cfb	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:26.066606998 CET	192.168.2.4	8.8.8.8	0x9154	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:31.331859112 CET	192.168.2.4	8.8.8.8	0xf7e3	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:36.613883972 CET	192.168.2.4	8.8.8.8	0xc0ff	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:41.885508060 CET	192.168.2.4	8.8.8.8	0x8c9f	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:47.394042969 CET	192.168.2.4	8.8.8.8	0xe2b9	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:52.678965092 CET	192.168.2.4	8.8.8.8	0xce24	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 20, 2021 09:30:58.011396885 CET	192.168.2.4	8.8.8.8	0x4db3	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 20, 2021 09:31:03.359149933 CET	192.168.2.4	8.8.8.8	0xd0b6	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)

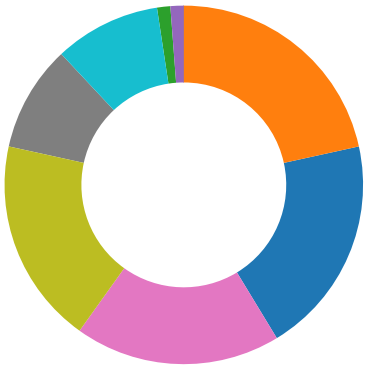
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 20, 2021 09:29:04.665582895 CET	8.8.8.8	192.168.2.4	0x373a	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:10.213303089 CET	8.8.8.8	192.168.2.4	0xf04d	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:15.782841921 CET	8.8.8.8	192.168.2.4	0x28b9	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:21.157784939 CET	8.8.8.8	192.168.2.4	0x92b2	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:26.478487015 CET	8.8.8.8	192.168.2.4	0x2f7d	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:31.760209084 CET	8.8.8.8	192.168.2.4	0x531a	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:37.038008928 CET	8.8.8.8	192.168.2.4	0x40e0	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:42.571342945 CET	8.8.8.8	192.168.2.4	0x45d	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:48.162168980 CET	8.8.8.8	192.168.2.4	0xe0fb	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:53.433005095 CET	8.8.8.8	192.168.2.4	0x32c9	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:29:58.705873013 CET	8.8.8.8	192.168.2.4	0x7bd0	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:04.296006918 CET	8.8.8.8	192.168.2.4	0x1d81	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:10.046027899 CET	8.8.8.8	192.168.2.4	0x2336	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:15.504040956 CET	8.8.8.8	192.168.2.4	0x6b7b	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:20.785655022 CET	8.8.8.8	192.168.2.4	0x1cfb	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:26.126811981 CET	8.8.8.8	192.168.2.4	0x9154	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:31.389084101 CET	8.8.8.8	192.168.2.4	0xf7e3	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:36.662565947 CET	8.8.8.8	192.168.2.4	0xc0ff	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:42.106175900 CET	8.8.8.8	192.168.2.4	0x8c9f	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:47.445638895 CET	8.8.8.8	192.168.2.4	0xe2b9	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:52.727715015 CET	8.8.8.8	192.168.2.4	0xce24	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:30:58.071069002 CET	8.8.8.8	192.168.2.4	0x4db3	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 20, 2021 09:31:03.584403038 CET	8.8.8.8	192.168.2.4	0xd0b6	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: CHEQUE COPY.exe PID: 6828 Parent PID: 5896

General

Start time:	09:28:56
Start date:	20/02/2021
Path:	C:\Users\user\Desktop\CHEQUE COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CHEQUE COPY.exe'
Imagebase:	0x400000
File size:	331665 bytes
MD5 hash:	EC067B73F3156AEDBD9158F107952EB8
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: 00000001.00000002.642106438.0000000002760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.642106438.0000000002760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.642106438.0000000002760000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.642106438.0000000002760000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsc691C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\l0k0ivt1gwq.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\mkecgmj.p	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\nsx694C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx694C.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx694C.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc691C.tmp	success or wait	1	40359C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsx694C.tmp	success or wait	1	4058CB	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\l0k0ivt1gwq.dll	unknown	10240	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 38 75 ef 62 59 1b bc 62 59 1b bc 62 59 1b bc 62 59 1a bc 74 59 1b bc 9e 2e a2 bc 6f 59 1b bc 45 9f d5 bc 63 59 1b bc 45 9f d1 bc 63 59 1b bc 45 9f d7 bc 63 59 1b bc 52 69 63 68 62 59 1b bc 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 50 45 00 00 4c 01 03 00 a1 6c 30 60 00 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 20 00 00 00 00 00	MZ.......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......&8u.bY..bY..bY..bY..t Y ......oY..E...cY..E...cY..E... cY..RichbY.................... ......PE..L....l0`...........!	success or wait	1	405D2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mkecgmj.p	unknown	32768	70 b3 4c 13 16 22 53 4c 3c b3 20 34 a8 93 fc cc f3 60 0c ed 94 c3 65 5c 16 27 82 53 96 9d 08 54 f5 34 7e 05 96 77 d3 25 4b 1d 6d 14 93 e3 03 8d 70 f2 50 cc d7 b9 0e d9 13 6c 3b 0d 72 a4 6e ec c2 7e a8 fc 5a 8e 33 29 93 ce 17 87 ff 0b bd 85 fa 52 97 f8 ed 23 dc 4a 96 22 59 59 8e 83 da 90 56 86 8d 27 93 8b 2f 04 1a 55 5e 75 a3 f0 42 01 3f 66 2a 2c 59 b8 ab a7 cd d9 32 88 1d 82 8c b5 9c 4f 65 42 1e 6b 2c d2 e8 af 2c 6d 8c 1a 5d 6c b1 fb 2a ca 9a 14 06 f5 b7 7b 7d 4a f3 59 35 7f 13 7f 87 6f f5 f1 25 67 ac f0 ce 7d e2 b0 61 26 e9 1f ca ec ff 73 30 a3 b4 2b 91 c1 3d 8d 3e 5e 84 9e 92 14 40 d6 7d c7 bc 84 40 eb 13 39 e4 54 db 39 0d 67 44 5c ca c5 3d 3a f2 34 1a 61 fb 90 2a 51 32 0f d0 99 e7 a7 6c db 65 0f 7c fa df 66 7b b6 58 f1 18 52 d1 43 2c 9d 6c e8 66 2b a8	p.L.."SL<. 4.....`....e\.'.S.. .T.4~..w.%K.m.....p.P......l;. r.n..~..Z.3).........R...#.J." YY....V..'../..U^u..B.?f*,Y... ..2......OeB.k,...,m..]l..*...... {}J.Y5....o..%g...}..a&.... .s0..+..=.>^....@.}...@..9.T. 9.gD\..=:.4.a..*Q2.....l.e.|..f {.X..R.C,.l.f+.	success or wait	9	405D2E	WriteFile
C:\Users\user\AppData\Local\Temp\nsx694C.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405D2E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CHEQUE COPY.exe	unknown	512	success or wait	71	405CFF	ReadFile
C:\Users\user\Desktop\CHEQUE COPY.exe	unknown	4	success or wait	2	405CFF	ReadFile
C:\Users\user\Desktop\CHEQUE COPY.exe	unknown	4	success or wait	14	405CFF	ReadFile
C:\Users\user\AppData\Local\Temp\mkecgmj.p	unknown	279040	success or wait	1	100044EE	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile

Analysis Process: CHEQUE COPY.exe PID: 6924 Parent PID: 6828

General

Start time:	09:28:56
Start date:	20/02/2021
Path:	C:\Users\user\Desktop\CHEQUE COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CHEQUE COPY.exe'
Imagebase:	0x400000
File size:	331665 bytes
MD5 hash:	EC067B73F3156AEDBD9158F107952EB8
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: 00000003.00000003.780327983.0000000000498000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000003.780327983.0000000000498000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000003.780327983.0000000000498000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.896985915.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.896985915.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.896985915.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.896985915.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000001.639777410.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000001.639777410.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000001.639777410.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000001.639777410.0000000000400000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000003.764460301.0000000000499000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000003.764460301.0000000000499000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000003.764460301.0000000000499000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.898053275.0000000002441000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.901950423.00000000058C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.901950423.00000000058C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.901950423.00000000058C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.901866159.0000000005820000.00000004.00000001.sdmp, Author:

	Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.901866159.0000000005820000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.898844721.00000000034BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.898844721.00000000034BC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.900532284.0000000004A62000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.900532284.0000000004A62000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.900532284.0000000004A62000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000003.742506685.0000000000499000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000003.742506685.0000000000499000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000003.742506685.0000000000499000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.899870723.0000000004920000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.899870723.0000000004920000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.899870723.0000000004920000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.899870723.0000000004920000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000003.789879813.0000000000499000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000003.789879813.0000000000499000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000003.789879813.0000000000499000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000003.709450530.0000000000499000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000003.709450530.0000000000499000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000003.709450530.0000000000499000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.897086081.0000000000489000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.897086081.0000000000489000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.897086081.0000000000489000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF4CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CF4CF06	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	6BD9BEFF	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	6BD91E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BD9BEFF	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	6BD9DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BD9DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BD97038	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	6BD91E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp811A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BD97038	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	6BD9BEFF	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	6BD9BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp	success or wait	1	6BD96A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp811A.tmp	success or wait	1	6BD96A95	DeleteFileW
C:\Users\user\Desktop\CHEQUE COPY.exe:Zone.Identifier	success or wait	1	5398BA6	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	79 d5 95 93 79 d5 d8 48	y...y..H	success or wait	1	6BD91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a8 21 81 40 ec 40 ef 13 ec 40 ef 13 ec 40 ef 13 2f 4f b0 13 ee 40 ef 13 ec 40 ee 13 4c 40 ef 13 2f 4f b2 13 e3 40 ef 13 b8 63 df 13 e0 40 ef 13 2b 46 e9 13 ed 40 ef 13 52 69 63 68 ec 40 ef 13 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 25 d6 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 64 00 00 00 b4 39 00 00 04 00 00 25 33 00 00 00 10 00 00 00 80 00 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........!.@.@...@...@../O... @ ...@..L@../O...@...c...@..+ F.. .@..Rich.@..........PE..L... %.$_.................d....9..... %3............@	success or wait	3	6BD9DD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6BD9DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp	unknown	1301	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	6BD91B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	38	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 43 48 45 51 55 45 20 43 4f 50 59 2e 65 78 65	C:\Users\user\Desktop\CH EQUE COPY.exe	success or wait	1	6BD91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp811A.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6BD91B4F	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	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD91B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CF0D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CF0D72F	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	6BD9646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 7096 Parent PID: 6924

General

Start time:	09:29:01
Start date:	20/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp'
Imagebase:	0xdc0000
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\tmp7DCD.tmp	unknown	2	success or wait	1	DCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7DCD.tmp	unknown	1302	success or wait	1	DCABD9	ReadFile

Analysis Process: conhost.exe PID: 7108 Parent PID: 7096

General

Start time:	09:29:02
Start date:	20/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 7148 Parent PID: 6924

General

Start time:	09:29:02
Start date:	20/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp811A.tmp'
Imagebase:	0xdc0000
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\tmp811A.tmp	unknown	2	success or wait	1	DCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp811A.tmp	unknown	1311	success or wait	1	DCABD9	ReadFile

Analysis Process: conhost.exe PID: 7164 Parent PID: 7148

General

Start time:	09:29:03
Start date:	20/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: CHEQUE COPY.exe PID: 6200 Parent PID: 968

General

Start time:	09:29:03
Start date:	20/02/2021
Path:	C:\Users\user\Desktop\CHEQUE COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CHEQUE COPY.exe' 0
Imagebase:	0x400000
File size:	331665 bytes
MD5 hash:	EC067B73F3156AEDBD9158F107952EB8
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: 0000000A.00000002.657465929.0000000002DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.657465929.0000000002DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.657465929.0000000002DB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.657465929.0000000002DB0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj85AD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj85AE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj85AE.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570A	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj85AE.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj85AD.tmp	success or wait	1	40359C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsj85AE.tmp	success or wait	1	4058CB	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\l0k0ivt1gwq.dll	unknown	10240	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 38 75 ef 62 59 1b bc 62 59 1b bc 62 59 1b bc 62 59 1a bc 74 59 1b bc 9e 2e a2 bc 6f 59 1b bc 45 9f d5 bc 63 59 1b bc 45 9f d1 bc 63 59 1b bc 45 9f d7 bc 63 59 1b bc 52 69 63 68 62 59 1b bc 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 50 45 00 00 4c 01 03 00 a1 6c 30 60 00 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 20 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......&8u.bY..bY..bY..bY..t Y ......oY..E...cY..E...cY..E... cY..RichbY................... ......PE..L....l0`...........!	success or wait	1	405D2E	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\mkecgmj.p</td><td>unknown</td><td>32768</td><td>70 b3 4c 13 16 22 53
4c 3c b3 20 34 a8 93
fc cc f3 60 0c ed 94 c3
65 5c 16 27 82 53 96
9d 08 54 f5 34 7e 05
96 77 d3 25 4b 1d 6d
14 93 e3 03 8d 70 f2
50 cc d7 b9 0e d9 13
6c 3b 0d 72 a4 6e ec
c2 7e a8 fc 5a 8e 33
29 93 ce 17 87 ff 0b bd
85 fa 52 97 f8 ed 23 dc
4a 96 22 59 59 8e 83
da 90 56 86 8d 27 93
8b 2f 04 1a 55 5e 75
a3 f0 42 01 3f 66 2a 2c
59 b8 ab a7 cd d9 32
88 1d 82 8c b5 9c 4f
65 42 1e 6b 2c d2 e8
af 2c 6d 8c 1a 5d 6c
b1 fb 2a ca 9a 14 06 f5
b7 7b 7d 4a f3 59 35 7f
13 7f 87 6f f5 f1 25 67
ac f0 ce 7d e2 b0 61
26 e9 1f ca ec ff 73 30
a3 b4 2b 91 c1 3d 8d
3e 5e 84 9e 92 14 40
d6 7d c7 bc 84 40 eb
13 39 e4 54 db 39 0d
67 44 5c ca c5 3d 3a f2
34 1a 61 fb 90 2a 51
32 0f d0 99 e7 a7 6c
db 65 0f 7c fa df 66 7b
b6 58 f1 18 52 d1 43
2c 9d 6c e8 66 2b a8</td><td>p.L.."SL<. 4.....`....e\.'.S..
.T.4~..w.%K.m.....p.P......l;.
r.n..~..Z.3).........R...#.J."
YY....V..'../..U^u..B.?f*,Y...
..2......OeB.k,...,m..]l..*......
{}J.Y5....o..%g...}..a&....
.s0..+..=.>^....@.}...@..9.T.
9.gD\..=:.4.a..*Q2.....l.e.|..f
{.X..R.C,.l.f+.</td><td>success or wait</td><td>9</td><td>405D2E</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsj85AE.tmp\System.dll</td><td>unknown</td><td>11776</td><td>4d 5a 90 00 03 00 00
00 04 00 00 00 ff ff 00
00 b8 00 00 00 00 00
00 00 40 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 d0 00 00 00
0e 1f ba 0e 00 b4 09
cd 21 b8 01 4c cd 21
54 68 69 73 20 70 72
6f 67 72 61 6d 20 63
61 6e 6e 6f 74 20 62
65 20 72 75 6e 20 69
6e 20 44 4f 53 20 6d 6f
64 65 2e 0d 0d 0a 24
00 00 00 00 00 00 00
69 72 2a 92 2d 13 44
c1 2d 13 44 c1 2d 13
44 c1 ae 0f 4a c1 2a
13 44 c1 2d 13 45 c1
3e 13 44 c1 ee 1c 19
c1 2a 13 44 c1 79 30
74 c1 29 13 44 c1 4e
31 6e c1 2c 13 44 c1
d2 33 40 c1 2c 13 44
c1 52 69 63 68 2d 13
44 c1 00 00 00 00 00
00 00 00 50 45 00 00
4c 01 04 00 a8 d5 24
5f 00 00 00 00 00 00
00 00 e0 00 2e 21 0b
01 06 00 00 20 00 00
00 0a 00 00 00 00 00
00 21 29 00 00 00 10
00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....$.......ir*.-.D.-.D.-
.D...J.*.D.-
.E.>.D.....*.D.y0t.).D.N1n.
,.D..3@.,.D.Rich-
.D.........PE
..L.....$_...........!..... ..
........!).....</td><td>success or wait</td><td>1</td><td>405D2E</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CHEQUE COPY.exe	unknown	512	success or wait	71	405CFF	ReadFile
C:\Users\user\Desktop\CHEQUE COPY.exe	unknown	4	success or wait	2	405CFF	ReadFile
C:\Users\user\Desktop\CHEQUE COPY.exe	unknown	4	success or wait	14	405CFF	ReadFile
C:\Users\user\AppData\Local\Temp\mkecgmj.p	unknown	279040	success or wait	1	100044EE	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile

Analysis Process: CHEQUE COPY.exe PID: 5852 Parent PID: 6200

General

Start time:	09:29:04
Start date:	20/02/2021
Path:	C:\Users\user\Desktop\CHEQUE COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CHEQUE COPY.exe' 0
Imagebase:	0x400000
File size:	331665 bytes
MD5 hash:	EC067B73F3156AEDBD9158F107952EB8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.672768392.000000000347C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.672768392.000000000347C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.670703063.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.670703063.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.670703063.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.670703063.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.674799984.0000000004FC2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.674799984.0000000004FC2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.674799984.0000000004FC2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.671006415.000000000055A000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.671006415.000000000055A000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.671006415.000000000055A000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000001.653978113.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000001.653978113.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000001.653978113.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.672627448.0000000002490000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.674570983.0000000004960000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.674570983.0000000004960000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.674570983.0000000004960000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.674570983.0000000004960000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.672690410.0000000003441000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.672690410.0000000003441000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.672690410.0000000003441000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF4CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CF4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CHEQUE COPY.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D25C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CHEQUE COPY.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D25C907	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	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD91B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6116 Parent PID: 968

General

Start time:	09:29:05
Start date:	20/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x400000
File size:	331665 bytes
MD5 hash:	EC067B73F3156AEDBD9158F107952EB8
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: 0000000C.00000002.676025735.0000000002E00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.676025735.0000000002E00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.676025735.0000000002E00000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.676025735.0000000002E00000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 45%, Virustotal, Browse • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsc8E96.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc8E96.tmp	success or wait	1	40359C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp	success or wait	1	4058CB	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\l0k0ivt1gwq.dll	unknown	10240	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 38 75 ef 62 59 1b bc 62 59 1b bc 62 59 1b bc 62 59 1a bc 74 59 1b bc 9e 2e a2 bc 6f 59 1b bc 45 9f d5 bc 63 59 1b bc 45 9f d1 bc 63 59 1b bc 45 9f d7 bc 63 59 1b bc 52 69 63 68 62 59 1b bc 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 50 45 00 00 4c 01 03 00 a1 6c 30 60 00 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 20 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......&8u.bY..bY..bY..bY..t Y ......oY..E...cY..E...cY..E... cY..RichbY.................... ......PE..L....l0`...........!	success or wait	1	405D2E	WriteFile
C:\Users\user\AppData\Local\Temp\mkecgmj.p	unknown	32768	70 b3 4c 13 16 22 53 4c 3c b3 20 34 a8 93 fc cc f3 60 0c ed 94 c3 65 5c 16 27 82 53 96 9d 08 54 f5 34 7e 05 96 77 d3 25 4b 1d 6d 14 93 e3 03 8d 70 f2 50 cc d7 b9 0e d9 13 6c 3b 0d 72 a4 6e ec c2 7e a8 fc 5a 8e 33 29 93 ce 17 87 ff 0b bd 85 fa 52 97 f8 ed 23 dc 4a 96 22 59 59 8e 83 da 90 56 86 8d 27 93 8b 2f 04 1a 55 5e 75 a3 f0 42 01 3f 66 2a 2c 59 b8 ab a7 cd d9 32 88 1d 82 8c b5 9c 4f 65 42 1e 6b 2c d2 e8 af 2c 6d 8c 1a 5d 6c b1 fb 2a ca 9a 14 06 f5 b7 7b 7d 4a f3 59 35 7f 13 7f 87 6f f5 f1 25 67 ac f0 ce 7d e2 b0 61 26 e9 1f ca ec ff 73 30 a3 b4 2b 91 c1 3d 8d 3e 5e 84 9e 92 14 40 d6 7d c7 bc 84 40 eb 13 39 e4 54 db 39 0d 67 44 5c ca c5 3d 3a f2 34 1a 61 fb 90 2a 51 32 0f d0 99 e7 a7 6c db 65 0f 7c fa df 66 7b b6 58 f1 18 52 d1 43 2c 9d 6c e8 66 2b a8	p.L.."SL<. 4.....`....e\.'.S.. .T.4~..w.%K.m.....p.P......l;. r.n..~..Z.3).........R...#.J." YY....V..'../..U^u..B.?f*,Y... ..2......OeB.k,...,m..]l..*...... {}J.Y5....o..%g...}..a&.... .s0..+..=.>^....@.}...@..9.T. 9.gD\..=:.4.a..*Q2.....l.e.|..f {.X..R.C,.l.f+.	success or wait	9	405D2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsvA2AC.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405D2E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	512	success or wait	71	405CFF	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	2	405CFF	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	14	405CFF	ReadFile
C:\Users\user\AppData\Local\Temp\mkecgmj.p	unknown	279040	success or wait	1	100044EE	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003849	ReadFile

Analysis Process: dhcpmon.exe PID: 6356 Parent PID: 6116

General

Start time:	09:29:12
Start date:	20/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x400000
File size:	331665 bytes
MD5 hash:	EC067B73F3156AEDBD9158F107952EB8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.688775764.00000000026C0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.688804869.0000000003671000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.688804869.0000000003671000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.688804869.0000000003671000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.687956985.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.687956985.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.687956985.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.687956985.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.688460054.00000000023F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.688460054.00000000023F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.688460054.00000000023F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.688460054.00000000023F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.689440306.0000000004A62000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.689440306.0000000004A62000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.689440306.0000000004A62000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000001.672061283.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000001.672061283.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000001.672061283.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.688856168.00000000036AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.688856168.00000000036AC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.688065638.00000000004BB000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.688065638.00000000004BB000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.688065638.00000000004BB000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF4CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CF4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D25C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D25C907	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	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD91B4F	ReadFile

Disassembly

Code Analysis