ID: 356453
Sample Name: PAYMENT COPY.exe
Cookbook: default.jbs
Time: 08:10:56
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

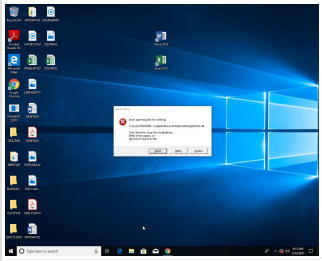
Analysis Report PAYMENT COPY.exe

Overview

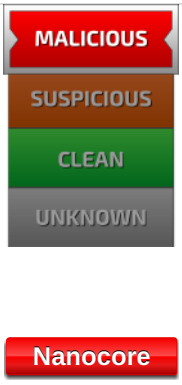
General Information

Sample Name:	PAYMENT COPY.exe
Analysis ID:	356453
MD5:	53e8c460446fe30.
SHA1:	bbebce3965dfc23..
SHA256:	b082aa828dd2eb..
Tags:	exe NanoCore RAT SCB

Most interesting Screenshot:



Detection



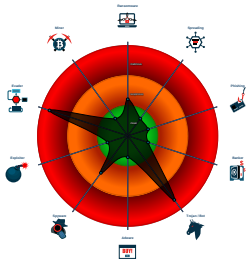
Nanocore

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**
- PAYMENT COPY.exe (PID: 6392 cmdline: 'C:\Users\user\Desktop\PAYMENT COPY.exe' MD5: 53E8C460446FE305DFC2159961AA6234)
  - PAYMENT COPY.exe (PID: 6432 cmdline: 'C:\Users\user\Desktop\PAYMENT COPY.exe' MD5: 53E8C460446FE305DFC2159961AA6234)
    - schtasks.exe (PID: 6532 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpEEDF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6596 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpF23B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PAYMENT COPY.exe (PID: 6612 cmdline: 'C:\Users\user\Desktop\PAYMENT COPY.exe' 0 MD5: 53E8C460446FE305DFC2159961AA6234)
  - PAYMENT COPY.exe (PID: 6712 cmdline: 'C:\Users\user\Desktop\PAYMENT COPY.exe' 0 MD5: 53E8C460446FE305DFC2159961AA6234)
- dhcpmon.exe (PID: 6744 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 53E8C460446FE305DFC2159961AA6234)
- dhcpmon.exe (PID: 5932 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 53E8C460446FE305DFC2159961AA6234)
  - dhcpmon.exe (PID: 2896 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 53E8C460446FE305DFC2159961AA6234)
- **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
00000001.00000002.498580778.000000000059 9000.00000004.00000020.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x29615:$x1: NanoCore.ClientPluginHost • 0x29652:$x2: IClientNetworkHost • 0x2d185:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.498580778.000000000059 9000.00000004.00000020.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.498580778.000000000059 9000.00000004.00000020.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2738:$a: NanoCore • 0x2937d:$a: NanoCore • 0x2938d:$a: NanoCore • 0x295c1:$a: NanoCore • 0x295d5:$a: NanoCore • 0x29615:$a: NanoCore • 0x293dc:$b: ClientPlugin • 0x295de:$b: ClientPlugin • 0x2961e:$b: ClientPlugin • 0x5fe50:$b: ClientPlugin • 0x79f06:$b: ClientPlugin • 0x29503:$c: ProjectData • 0x29f0a:$d: DESCrypto • 0x318d6:$e: KeepAlive • 0x2f8c4:$g: LogClientMessage • 0x2babf:$i: get_Connected • 0x2a240:$j: #=q • 0x2a270:$j: #=q • 0x2a28c:$j: #=q • 0x2a2bc:$j: #=q • 0x2a2d8:$j: #=q
00000001.00000002.500337236.000000000073 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
00000001.00000002.500337236.000000000073 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost

Click to see the 113 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.PAYMENT COPY.exe.780000.16.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost
1.2.PAYMENT COPY.exe.780000.16.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5fee:$x2: NanoCore.ClientPluginHost • 0x9441:$s4: PipeCreated • 0x6018:$s5: IClientLoggingHost
1.2.PAYMENT COPY.exe.27b2a64.22.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1deb:$x1: NanoCore.ClientPluginHost • 0x1e24:$x2: IClientNetworkHost
1.2.PAYMENT COPY.exe.27b2a64.22.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1deb:$x2: NanoCore.ClientPluginHost • 0x1f36:$s4: PipeCreated • 0x1e05:$s5: IClientLoggingHost
1.2.PAYMENT COPY.exe.400000.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x251e5:$x1: NanoCore.ClientPluginHost • 0x25222:$x2: IClientNetworkHost • 0x28d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 337 entries				

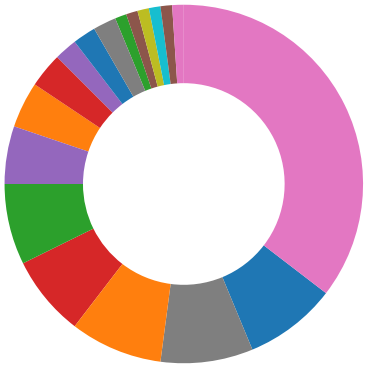
Sigma Overview

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
- Lowering of HIPS / PFW / Operating System Security Settings
- 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)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

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

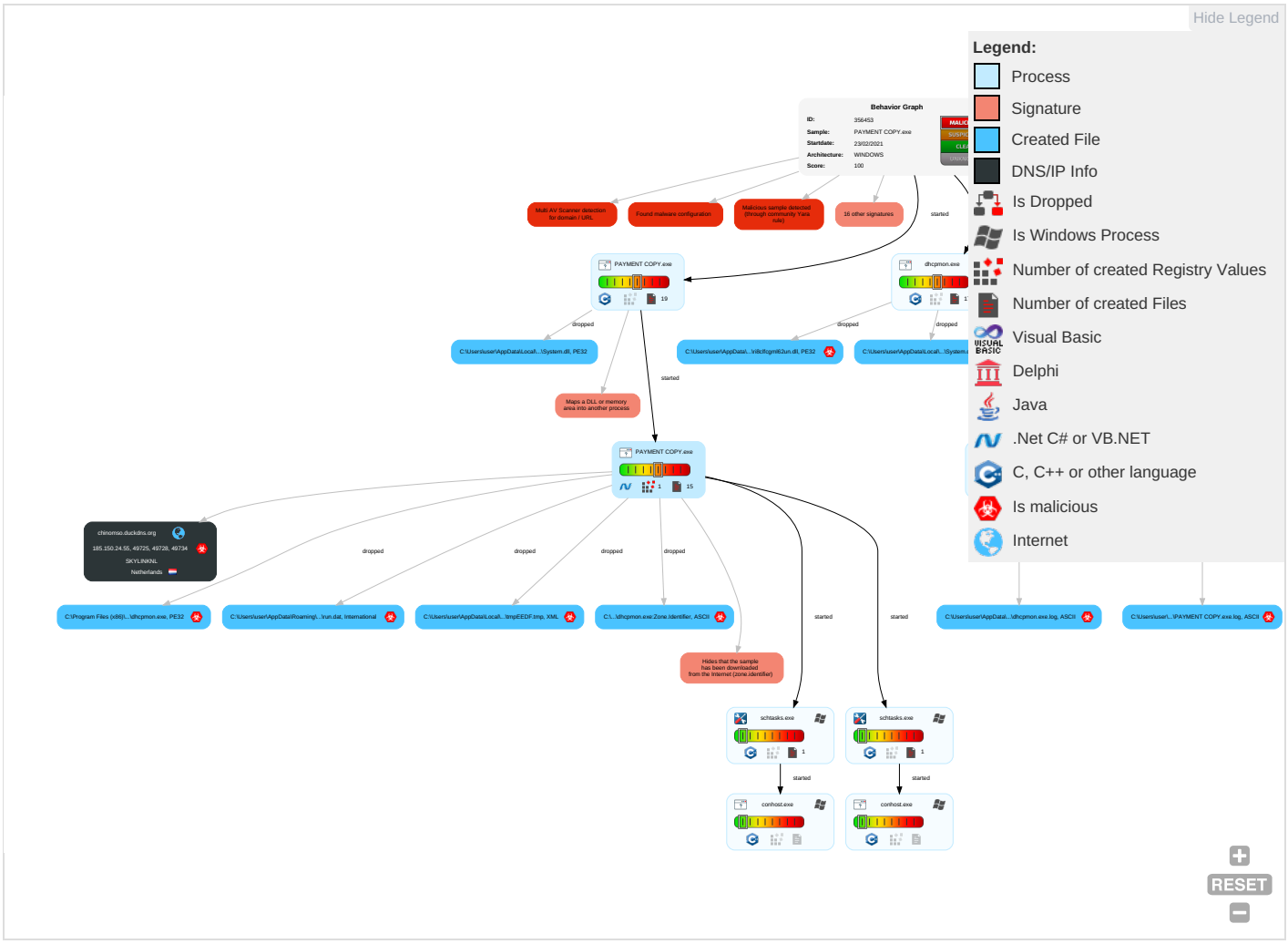
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 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
Default Accounts	Native API 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
Domain Accounts	Scheduled Task/Job 1	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 2	NTDS	Security Software Discovery 1 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
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
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
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
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
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

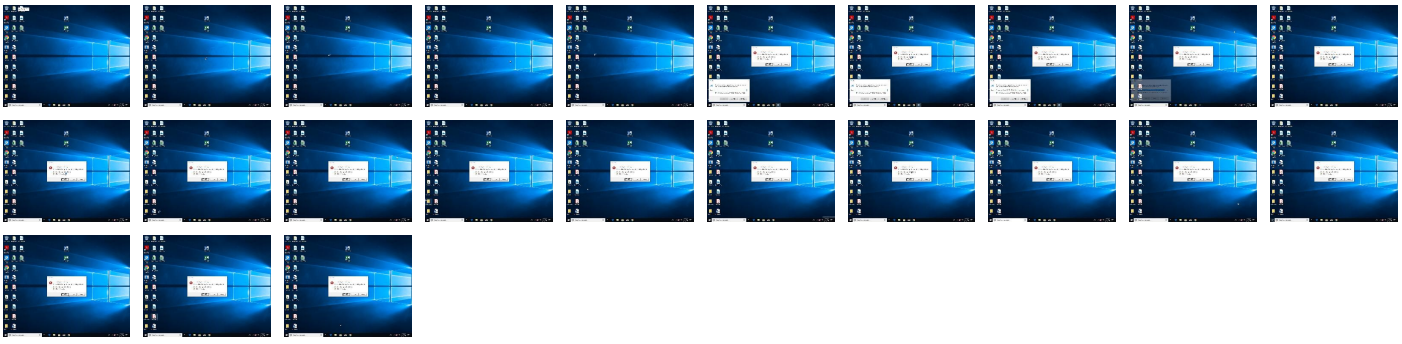
Behavior Graph



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
PAYMENT COPY.exe	35%	ReversingLabs	Win32.Backdoor.Androm	
PAYMENT 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	35%	ReversingLabs	Win32.Backdoor.Androm	
C:\Users\user\AppData\Local\Temp\nsc2504.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsc2504.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsc2504.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsmD8C8.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsmD8C8.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsoF70E.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsoF70E.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\ri8clfcgml62un.dll	15%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.PAYMENT COPY.exe.342c1f8.24.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.dhcpmon.exe.4e30000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
8.1.PAYMENT COPY.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.1.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
14.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
10.2.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
10.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
15.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.PAYMENT COPY.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.1.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
7.2.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
8.2.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.PAYMENT COPY.exe.49c0000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.0.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		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

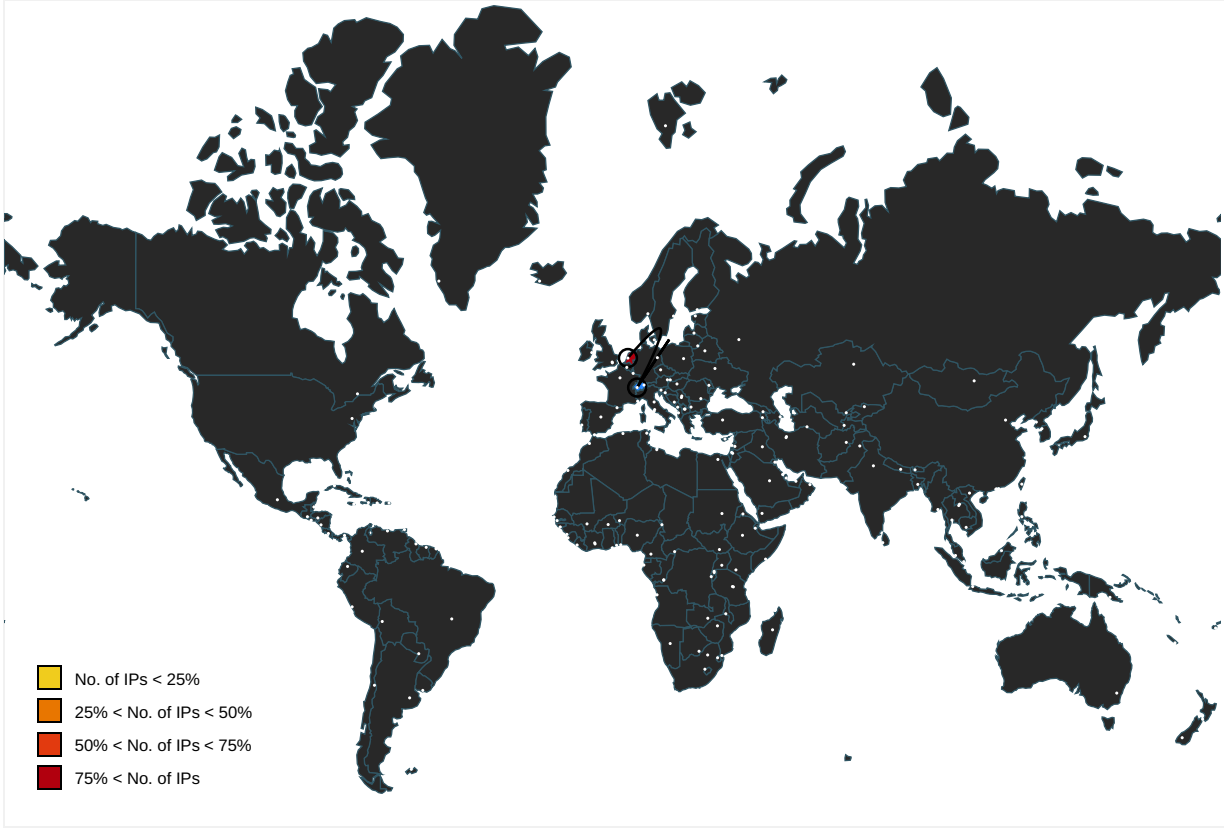
Contacted URLs

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	dhcpmon.exe, dhcpmon.exe, 0000000A.00000002.497269393.000000000040A000.00000004.00020000.sdmp, dhcpmon.exe, 0000000E.00000000.270226951.000000000040A000.00000008.00020000.sdmp, dhcpmon.exe, 0000000F.00000000.273721399.000000000040A000.00000008.00020000.sdmp, PAYMENT COPY.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	PAYMENT 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:	356453
Start date:	23.02.2021
Start time:	08:10:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT 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:	36
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@16/24@13/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 17.6% (good quality ratio 16.6%) • Quality average: 79.1% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 87% • 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, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.132.208.181, 13.64.90.137, 92.122.145.220, 104.42.151.234, 168.61.161.212, 184.30.20.56, 51.104.144.132, 51.103.5.159, 93.184.221.240, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:11:56	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\PAYMENT COPY.exe" s>$(Arg0)
08:11:56	API Interceptor	1004x Sleep call for process: PAYMENT COPY.exe modified
08:11:58	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Time	Type	Description
08:11:59	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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\nsc2504.tmp\System.dll	Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	
	INV_PR2201.docm	Get hash	malicious	Browse	
	CV-JOB REQUEST_____PDF.EXE	Get hash	malicious	Browse	
	Request for Quotation.exe	Get hash	malicious	Browse	
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	
	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	
	quote.exe	Get hash	malicious	Browse	
	Order83930.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	GPP.exe	Get hash	malicious	Browse	
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	
	ACCOUNT DETAILS.exe	Get hash	malicious	Browse	
	Quotation.com.exe	Get hash	malicious	Browse	
	Unterlagen PDF.exe	Get hash	malicious	Browse	
	QuotationInvoices.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.FileRepMalware.24882.exe	Get hash	malicious	Browse	
	PDF_doc.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	332412
Entropy (8bit):	7.946662165967432
Encrypted:	false
SSDEEP:	6144:S11QoY9YMstdr55cZ+TsUHBL5xY9j2DLWkl3TsJxdxEn7mZ:+Yxk55cZ+NhL5i9SWkRIjdxBZ
MD5:	53E8C460446FE305DFC2159961AA6234
SHA1:	BBEBCE3965DFC237EAC2711A47C141A4F8FF0083
SHA-256:	B082AA828DD2EB42D6E1DE8CCD8573AC3096CEEE92AD26449FC1DF6E490FF4ED
SHA-512:	4043358BEFD7A7FAC79C6E244FC8ADB6CA0F61E1F1B8427875455AE82E3DF47EA982467BB2C993D4C6EAD382F2A3DA77FAFFEF96E53712A393C12445E07F01E2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L..._.$_.....f...x.....4.....@.....@.....D.....`..... .....text....e.....f..... ..`.rdata.....j.....@..@.data...XU.....~.....@....ndata.....rsrc...`.....@..@..... ....

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

Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Encrypted:	false
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\PAYMENT COPY.exe.log	
Process:	C:\Users\user\Desktop\PAYMENT 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\extndbrvvs.aly	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	279040
Entropy (8bit):	**7.999355482654256**
Encrypted:	**true**
SSDEEP:	6144:SGrQWot55cT+FsUHBL5xy9j2DL+kl3ZsJx1xEnwXSIIV:SGBg55cT+zhL5A9S+kRmj1xpSIO
MD5:	CD58A93032A5720ED2F2E6DD9F615956
SHA1:	9CC17C0944B7124758E59842E59634EFDE088443

C:\Users\user\AppData\Local\Temp\extndbrvvs.aly	
SHA-256:	FA902D29A67B5890704B4B05CF3EE1F3ECF3ED37BE037BE70B0943FA367D1C12
SHA-512:	9250A73290622C574D12E68417069A34329AB7D3F4F161D2F0A426814912CF0EB568E4EAB95EB3992A8B18192FDDF9BA895D250BA7C12AC526EA7D157EECC83
Malicious:	false
Preview:	k.....")3..Nf.YQ.e.....l..-..U.c.E%..nq.O...O.o,.ef.....K.R'.j,..I(..X.a(.)9;.c..].L.Q....b...Or....c..>zS1."R.6.?@g...).n'.{o.....b..L.~`.Ew..i-..R.L.M..=.C...Q.6.Se.'.h.o.. I..a. +..@...m3.....M. .....x=x...}.@..6...n....>..]]6....h.Z.0_..v..v .G..h..0.-....(.[N.I....dp.....['r.rWz .Mu..[.6.....:fsL....S.....v.C.&0Q+pSMo`.DC)`..#...1j..<....=.....Rt.i..Y..m.5X...0 .X..W.....m.cf...3.P@./R.=....v.%.-.=Fp..hU_..7 .n...Y."7}i6Csw).H....Ic.a..s.m.[....|.P...../I....z.....1..'...../K.....1.....(.i..6.I.....b~/z..M....W.....:0.I...+.....?....RC. Yu46...Z(.9[]..|..%.....G..}....~....?...N..h.O...|..m*Q...>Ux.l5.K..M..T&...EA>.C.I.%.>.be.z.N..-E.k.....&...>... o..0/[(.....J...xA....:h!.{n*.....R.+.v.BGs".8.....|...+M^ .R...1t.$.....yC....tk.d...#...Z..K...Y0...3.R..`..ZY...f_.....z.0..\.Q....e..h..,$...R. .....5<..D...".\{.~.";.1...T.z.....W../zs.s...8.../D%KXu....x.....v.+.t.&L.....Q.

C:\Users\user\AppData\Local\Temp\nsc2504.tmp\System.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
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: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe, Detection: malicious, Browse • Filename: INV_PR2201.docm, Detection: malicious, Browse • Filename: CV-JOB REQUEST_____PDF.EXE, Detection: malicious, Browse • Filename: Request for Quotation.exe, Detection: malicious, Browse • Filename: #U007einvoice#U007eSC00978656.xlsx, Detection: malicious, Browse • Filename: Purchase Order___pdf _____.exe, Detection: malicious, Browse • Filename: quote.exe, Detection: malicious, Browse • Filename: Order83930.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: GPP.exe, Detection: malicious, Browse • Filename: OrderSuppliesQuote0817916.exe, Detection: malicious, Browse • Filename: ACCOUNT DETAILS.exe, Detection: malicious, Browse • Filename: Quotation.com.exe, Detection: malicious, Browse • Filename: Unterlagen PDF.exe, Detection: malicious, Browse • Filename: QuotationInvoices.exe, Detection: malicious, Browse • Filename: PO.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.FileRepMalware.24882.exe, Detection: malicious, Browse • Filename: PDF_doc.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\nsm24A5.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	306118
Entropy (8bit):	7.939787418337237
Encrypted:	false
SSDEEP:	6144:AtyGrQWot55cT+FsUHBL5xy9j2DL+kl3ZsJx1xEnwXSIIYt:QyGBg55cT+zhL5A9S+kRmj1xpSIH
MD5:	9B39D5926D9633B180D4AFB3E7CAAC40
SHA1:	06D5F9B6111F68E35F40A1AA609271F000DA23F1
SHA-256:	FFE073951D33F7DE224C4892F4EDE7B7368C9A37589263BB73D0B87014CF8D96
SHA-512:	D0FDA76963586867DCE03AEAE079EEB943EEF56776B909E239EB97200DFA8742F421C342D80D0617528527EF9E10C1869CFEAC8F3078A0F084368DFCC11FD05
Malicious:	false
Preview:	.....,.....$..... .....J.....,...j..... ....

C:\Users\user\AppData\Local\Temp\nsmD8C8.tmp\System.dll	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe

C:\Users\user\AppData\Local\Temp\nsmD8C8.tmp\System.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
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\nsn16.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	modified
Size (bytes):	22347
Entropy (8bit):	6.772137166768519
Encrypted:	false
SSDEEP:	384:A9QcELMTSkCWlpxuWR0O+mGS83jurV4pa4bg+T40K:AMLMukLPxuk3yp3K
MD5:	904BE663881896399EC80434BA4AFC15
SHA1:	FB5000F7CC9F3248EC9958E35704E60650A58B59
SHA-256:	9FD0A2635122A785EF88BE78C820EC044A90CFCD44CD8810EC09C736E160B4E8
SHA-512:	96100AAE73825DC66CEF953232E34744FB2451812CD2B85EDDDCC4FB8DE3FB81FF672B68AE57E82B3B3CA7B14CA56671035A640B1778B915E684DEEFAEFE4A5E
Malicious:	false
Preview:	.....,.....$..... .....J.....,...j..... ....

C:\Users\user\AppData\Local\Temp\nsoF70E.tmp\System.dll	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
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\nsuF6DF.tmp	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	data
Category:	dropped
Size (bytes):	306118
Entropy (8bit):	7.939787418337237
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nsuF6DF.tmp	
SSDEEP:	6144:AtyGrQWot55cT+FsUHBL5xy9j2DL+kl3ZsJx1xEnwXSIIYt:QyGBg55cT+zhL5A9S+kRmj1xpSIH
MD5:	9B39D5926D9633B180D4AFB3E7CAAC40
SHA1:	06D5F9B6111F68E35F40A1AA609271F000DA23F1
SHA-256:	FFE073951D33F7DE224C4892F4EDE7B7368C9A37589263BB73D0B87014CF8D96
SHA-512:	D0FDA76963586867DCE03AEAE079EEB943EEF56776B909E239EB97200DFA8742F421C342D80D0617528527EF9E10C1869CFEAC8F3078A0F084368DFCC11FD05
Malicious:	false
Preview:	.....,.....$..... .....J.....,...j..... ....

C:\Users\user\AppData\Local\Temp\nsxD899.tmp	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	data
Category:	dropped
Size (bytes):	306118
Entropy (8bit):	7.939787418337237
Encrypted:	false
SSDEEP:	6144:AtyGrQWot55cT+FsUHBL5xy9j2DL+kl3ZsJx1xEnwXSIIYt:QyGBg55cT+zhL5A9S+kRmj1xpSIH
MD5:	9B39D5926D9633B180D4AFB3E7CAAC40
SHA1:	06D5F9B6111F68E35F40A1AA609271F000DA23F1
SHA-256:	FFE073951D33F7DE224C4892F4EDE7B7368C9A37589263BB73D0B87014CF8D96
SHA-512:	D0FDA76963586867DCE03AEAE079EEB943EEF56776B909E239EB97200DFA8742F421C342D80D0617528527EF9E10C1869CFEAC8F3078A0F084368DFCC11FD05
Malicious:	false
Preview:	.....,.....$..... .....J.....,...j..... ....

C:\Users\user\AppData\Local\Temp\ri8clfcgml62un.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):	6.617616566986233
Encrypted:	false
SSDEEP:	192:l1fAHxDSLwXELMtO5KwHXYHCWxDpJL0jWP3p0Oy:cQcELMTSkCWlpxuWR0O
MD5:	19ACEBD18CD8160A4835FF53469C479B
SHA1:	486432D9B1752D28D79ACDC037CB54569B83C05D
SHA-256:	359038B41761F6903B97E9B51DC35C062D4D253AF628BEACBAE79A7D44CF1F22
SHA-512:	C010B18F028600BC60AE8993690A5142D1CFA23E0AC1C9E8DBFC3974F08E708B8A5F16AFB8633AE16736BC79018A85F2855DF10DEC93356713C5C6235F1CB5E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.N.e.N.e.N.e.N.e.NI..N.e.N..cN.e.N..gN.e.N..dN.e.N..aN.e .NRich.e.N.....PE..L...dx4`.....!.....&..... .....p.....@.....P$..I.... .....P.....`..d..... .....code...L..... ....rdata..... .....@..@.data.....0.....@....rsrc.....P.....*.....@..@.reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tmpEEDF.tmp	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1306
Entropy (8bit):	5.1109020496994875
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0A+Pp8xtn:cbk4oL600QydbQxIYODOLedq3vqp8j
MD5:	AFDDA7F0503E444134BC1A8B7DFCB5FD
SHA1:	9C9EBEE89239A89C3FD750B123DC528B98E38198
SHA-256:	70317BDEB4DD67C116F85C43427A2EC7369B60DC53B323B9C0897FFAC9E9A027
SHA-512:	B5FAF6350AB75EAC644059C1B6D9E09A4550BD609DBA55ED7DB22C95DD58D4112274629BC10E17B1D35C8555D012CA949EDEF1235BF4FB2DC79323EAAC3A1 F3
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmpEEDF.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpF23B.tmp	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	data
Category:	dropped
Size (bytes):	928
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtw:Ik/lCrwfk/lCrwfk/lCrwfk/lCrw8
MD5:	CCB690520E68EE385ACC0ACFE759AFFC
SHA1:	33F0DA3F55E5B3C5AC19B61D31471CB60BCD5C96
SHA-256:	166154225DAB5FCB79C1CA97D371B159D37B83FBC0ADABCD8EBA98FA113A7A3B
SHA-512:	AC4F3CF1F8F460745D37E6350861C2FBCDDCC1BBDE0A48FB361BFBF5B1EBF10A05F798A72CE413FCA073FF8108955353DDBCBD9D50CED6CDAE231C67A28FDA3
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	International EBCDIC text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.4056390622295662
Encrypted:	false
SSDEEP:	3:0I:0I
MD5:	3CBBBAC199963ABCF4667B290F5BC226
SHA1:	EF2F3B0E7DF4A2DAEDD2BEF311FBAB7F5C651DE0
SHA-256:	0C8B09A6E62621A09F742CDC38DB8DC94B247E678DE264A99DAA216EB461087F
SHA-512:	9E66F75D4907FACD9484986E87D63ECEC7BDCF4EBC2ACA55B4DF5073BFF6FF2A01527C65ED7A6C2A44444C2D4EFCB26D233CEEBCA7B2074AC3387BB67EA15C1
Malicious:	**true**
Preview:	p.....H

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..l..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	4.458598697157055
Encrypted:	false
SSDEEP:	3:oN0naRR1k+PaAdA:oNcSRu+PpA
MD5:	AC74F0849FB911B24DEBB2AEDEE8E24C
SHA1:	8797005CAE13E840F2E14E0F787ADA26F24DD32F
SHA-256:	BBF827B7252E76C927747FE8875F19392D54C070CB743DDE37095715705D0C7B
SHA-512:	DB156C220C174959351DA1F8D1402AADB261D4383EDDE9297D534F92127680D39E78A177DD271CBF8F7255E199A4963EC896A06AF1A439174AE8E909DD9F9D8
Malicious:	false
Preview:	C:\Users\user\Desktop\PAYMENT COPY.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.946662165967432
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:	PAYMENT COPY.exe

General

File size:	332412
MD5:	53e8c460446fe305dfc2159961aa6234
SHA1:	bbebce3965dfc237eac2711a47c141a4f8ff0083
SHA256:	b082aa828dd2eb42d6e1de8ccd8573ac3096ceee92ad26449fc1df6e490ff4ed
SHA512:	4043358befd7a7fac79c6e244fc8adb6ca0f61e1f1b8427875455ae82e3df47ea982467bb2c993d4c6ead382f2a3da77faffef96e53712a393c12445e07f01b2
SSDEEP:	6144:S11QoY9YMstdr55cZ+TsUHBL5xY9j2DLWkl3TsJxdxEn7mZ:+Yxk55cZ+NhL5i9SWkRIjdxBZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..._.$_.....f...x.....4.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403486
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:	0x5F24D75F [Sat Aug 1 02:45:51 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:	ea4e67a31ace1a72683a99b80cf37830

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], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F44Ch], eax
je 00007FF014AB6A83h
push ebx
call 00007FF014AB9BFEh
cmp eax, ebx
je 00007FF014AB6A79h

Instruction
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007FF014AB9B7Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FF014AB6A5Dh
push 0000000Bh
call 00007FF014AB9BD2h
push 00000009h
call 00007FF014AB9BCBh
push 00000007h
mov dword ptr [0042F444h], eax
call 00007FF014AB9BBFh
cmp eax, ebx
je 00007FF014AB6A81h
push 0000001Eh
call eax
test eax, eax
je 00007FF014AB6A79h
or byte ptr [0042F44Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F518h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429878h
call dword ptr [0040816Ch]
push 0040A1ECh

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	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x960	.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	0x65ad	0x6600	False	0.675628063725	data	6.48593060343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4634765625	data	5.26110074066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25558	0x600	False	0.470052083333	data	4.21916068772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x960	0xa00	False	0.4484375	data	4.27028215028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x38148	0x100	data	English	United States
RT_DIALOG	0x38248	0x11c	data	English	United States
RT_DIALOG	0x38364	0x60	data	English	United States
RT_VERSION	0x383c4	0x25c	data	English	United States
RT_MANIFEST	0x38620	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
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, 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 Shaanxi
FileVersion	90.50.10.2
CompanyName	symbolic
LegalTrademarks	Buol
Comments	Saxony
ProductName	lightbulb
FileDescription	survivor
Translation	0x0409 0x04e4

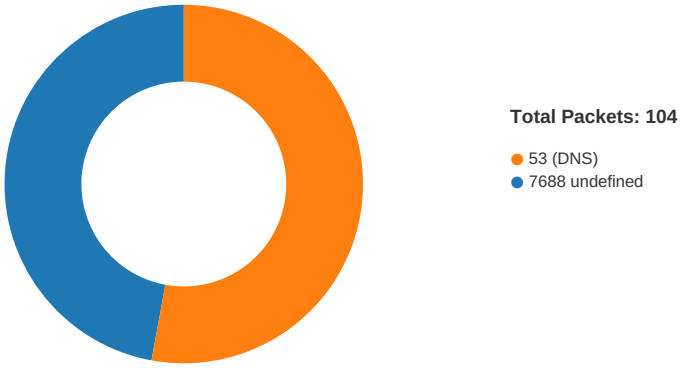
Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:11:57.971867085 CET	49711	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:01.054852962 CET	49711	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:07.061415911 CET	49711	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:17.394999981 CET	49725	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:20.453207016 CET	49725	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:26.453692913 CET	49725	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:35.758625984 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:38.751656055 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:39.653305054 CET	7688	49725	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:39.653495073 CET	49725	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:40.105993032 CET	7688	49725	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:44.923953056 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:45.132733107 CET	7688	49728	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:45.132883072 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:45.176296949 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:45.396951914 CET	7688	49728	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:45.410798073 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:45.616755009 CET	7688	49728	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:45.720943928 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:45.939094067 CET	7688	49728	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:45.967158079 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:46.128530025 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:46.329687119 CET	7688	49728	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:46.329785109 CET	49728	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:50.471874952 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:50.676709890 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:50.676826000 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:50.677452087 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:50.900098085 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:50.902806997 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.103795052 CET	7688	49734	185.150.24.55	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:12:51.107040882 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.396121025 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.400945902 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.425412893 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.426062107 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.437114000 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.443243980 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.444075108 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.448003054 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.448935032 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.449178934 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.643914938 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.652127981 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.653007030 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.663764954 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.673142910 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.674065113 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.677896976 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.683335066 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.685416937 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.690367937 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.696141958 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.705013037 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.866880894 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.874144077 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.874244928 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.882159948 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.891952991 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.892081022 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.904917002 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.913801908 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.913990021 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.923981905 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.934052944 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.934134960 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.941858053 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.951328039 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.951500893 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.970124006 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.975358963 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:51.975538015 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:51.990825891 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.005896091 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.005975008 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.044104099 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.073807955 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.073971033 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.128669024 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.155844927 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.155997992 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.166887045 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.174671888 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.174772978 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.175527096 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.181725979 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.181843042 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.188837051 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.188988924 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.203799009 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.203965902 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.216903925 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.217087984 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.240864038 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.241003036 CET	49734	7688	192.168.2.7	185.150.24.55

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:12:52.251765966 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.251950026 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.270746946 CET	7688	49734	185.150.24.55	192.168.2.7
Feb 23, 2021 08:12:52.270845890 CET	49734	7688	192.168.2.7	185.150.24.55
Feb 23, 2021 08:12:52.281265974 CET	7688	49734	185.150.24.55	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:11:41.903371096 CET	58562	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:41.949830055 CET	56590	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:41.955261946 CET	53	58562	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:41.998357058 CET	53	56590	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:42.129158974 CET	60501	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:42.177692890 CET	53	60501	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:43.701062918 CET	53775	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:43.753017902 CET	53	53775	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:44.062700033 CET	51837	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:44.123857975 CET	53	51837	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:45.027590036 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:45.078006029 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:46.430269957 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:46.480618954 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:47.605781078 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:47.654464006 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:48.597007036 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:48.645579100 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:49.554630995 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:49.603455067 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:50.859311104 CET	58717	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:50.908116102 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:52.048846960 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:52.100598097 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:53.974230051 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:54.034193993 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:55.835946083 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:55.885308027 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:57.696343899 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:57.916781902 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:58.103384972 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:58.154814959 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 08:11:59.633799076 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:11:59.682451963 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:01.157835007 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:01.206501007 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:02.868599892 CET	52816	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:02.920520067 CET	53	52816	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:04.380520105 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:04.432784081 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:06.958430052 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:07.018827915 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:07.152877092 CET	54911	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:07.201458931 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:08.184039116 CET	49958	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:08.235394001 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:09.404309988 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:09.458390951 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:11.257404089 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:11.316282988 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:12.615478992 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:12.664199114 CET	53	59730	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:17.166829109 CET	59310	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:17.393465996 CET	53	59310	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:19.701574087 CET	51919	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:12:19.751816988 CET	53	51919	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:35.698424101 CET	64296	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:35.756969929 CET	53	64296	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:37.144649982 CET	56680	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:37.156831980 CET	58820	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:37.194583893 CET	53	56680	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:37.218147993 CET	53	58820	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:39.933470964 CET	60983	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:39.986462116 CET	53	60983	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:50.250233889 CET	49247	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:50.470235109 CET	53	49247	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:52.268327951 CET	52286	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:52.326889038 CET	53	52286	8.8.8.8	192.168.2.7
Feb 23, 2021 08:12:57.225146055 CET	56064	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:12:57.453453064 CET	53	56064	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:05.064574003 CET	63744	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:05.124604940 CET	53	63744	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:11.557959080 CET	61457	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:11.619239092 CET	53	61457	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:14.104386091 CET	58367	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:14.164246082 CET	53	58367	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:14.823729992 CET	60599	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:14.880944014 CET	53	60599	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:15.617856026 CET	59571	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:15.668433905 CET	53	59571	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:16.447695971 CET	52689	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:16.506561041 CET	53	52689	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:16.961836100 CET	50290	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:17.023086071 CET	53	50290	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:17.515580893 CET	60427	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:17.567055941 CET	53	60427	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:19.216253996 CET	56209	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:19.273304939 CET	53	56209	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:19.680048943 CET	59582	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:19.737291098 CET	53	59582	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:20.464555025 CET	60949	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:20.524211884 CET	53	60949	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:21.624974012 CET	58542	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:21.673666954 CET	53	58542	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:22.570275068 CET	59179	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:22.629508018 CET	53	59179	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:23.264425993 CET	60927	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:23.312992096 CET	53	60927	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:25.127729893 CET	57854	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:25.187793970 CET	53	57854	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:31.232362986 CET	62026	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:31.459999084 CET	53	62026	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:38.460644007 CET	59453	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:38.522447109 CET	53	59453	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:41.938846111 CET	62468	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:41.987490892 CET	53	62468	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:44.666580915 CET	52563	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:44.715342045 CET	53	52563	8.8.8.8	192.168.2.7
Feb 23, 2021 08:13:52.423085928 CET	54721	53	192.168.2.7	8.8.8.8
Feb 23, 2021 08:13:52.484493017 CET	53	54721	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:11:57.696343899 CET	192.168.2.7	8.8.8.8	0x433	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:17.166829109 CET	192.168.2.7	8.8.8.8	0xd7ab	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:35.698424101 CET	192.168.2.7	8.8.8.8	0x3462	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:12:50.250233889 CET	192.168.2.7	8.8.8.8	0x992d	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:57.225146055 CET	192.168.2.7	8.8.8.8	0xfb0b	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:05.064574003 CET	192.168.2.7	8.8.8.8	0x28a8	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:11.557959080 CET	192.168.2.7	8.8.8.8	0x1f5d	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:19.216253996 CET	192.168.2.7	8.8.8.8	0x6412	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:25.127729893 CET	192.168.2.7	8.8.8.8	0xafc5	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:31.232362986 CET	192.168.2.7	8.8.8.8	0xb242	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:38.460644007 CET	192.168.2.7	8.8.8.8	0x8293	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:44.666580915 CET	192.168.2.7	8.8.8.8	0x1e5	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:52.423085928 CET	192.168.2.7	8.8.8.8	0xbe7c	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)

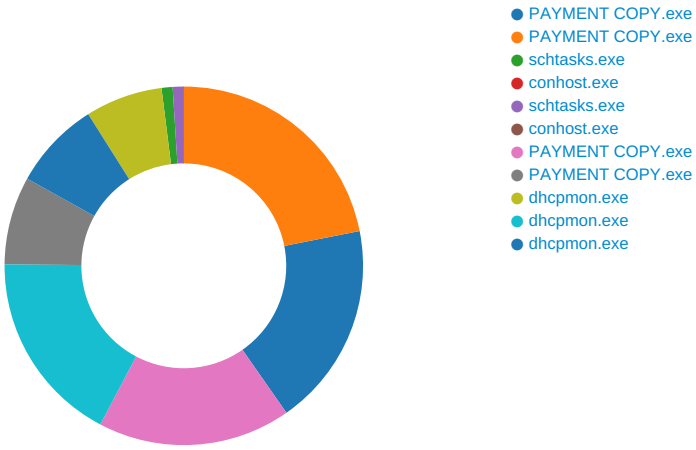
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:11:57.916781902 CET	8.8.8.8	192.168.2.7	0x433	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:17.393465996 CET	8.8.8.8	192.168.2.7	0xd7ab	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:35.756969929 CET	8.8.8.8	192.168.2.7	0x3462	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:50.470235109 CET	8.8.8.8	192.168.2.7	0x992d	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:57.453453064 CET	8.8.8.8	192.168.2.7	0xfb0b	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:05.124604940 CET	8.8.8.8	192.168.2.7	0x28a8	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:11.619239092 CET	8.8.8.8	192.168.2.7	0x1f5d	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:19.273304939 CET	8.8.8.8	192.168.2.7	0x6412	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:25.187793970 CET	8.8.8.8	192.168.2.7	0xafc5	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:31.459999084 CET	8.8.8.8	192.168.2.7	0xb242	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:38.522447109 CET	8.8.8.8	192.168.2.7	0x8293	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:44.715342045 CET	8.8.8.8	192.168.2.7	0x1e5	No error (0)	chinomso.duckdns.org		185.150.24.55	A (IP address)	IN (0x0001)
Feb 23, 2021 08:13:52.484493017 CET	8.8.8.8	192.168.2.7	0xbe7c	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: PAYMENT COPY.exe PID: 6392 Parent PID: 5664

General

Start time:	08:11:48
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PAYMENT COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT COPY.exe'
Imagebase:	0x400000
File size:	332412 bytes
MD5 hash:	53E8C460446FE305DFC2159961AA6234
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: 00000000.00000002.242328677.0000000002A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.242328677.0000000002A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.242328677.0000000002A80000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.242328677.0000000002A80000.00000004.00000001.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~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsxD869.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\nsxD899.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	CreateDirectoryA
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\ri8clfcgml62un.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user~1\AppData\Local\Temp\extndbrvvs.aly	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user~1\AppData\Local\Temp\nsmD8C8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	CreateDirectoryA
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsmD8C8.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	405883	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsmD8C8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxD869.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsmD8C8.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxD899.tmp	unknown	22347	b6 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 f0 0c 00 00 01 00 00 00 b6 0d 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,..................$.	success or wait	19	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\ri8clfcgml62un.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 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 f1 04 c3 1d b5 65 ad 4e b5 65 ad 4e b5 65 ad 4e b5 65 ac 4e 9f 65 ad 4e 49 12 14 4e ba 65 ad 4e 92 a3 63 4e b4 65 ad 4e 92 a3 67 4e b4 65 ad 4e 92 a3 64 4e b4 65 ad 4e 92 a3 61 4e b4 65 ad 4e 52 69 63 68 b5 65 ad 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 64 78 34 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 26 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............e.N.e.N.e.N.e.N.e .NI..N.e.N..cN.e.N..gN.e.N. .dN .e.N..aN.e.NRich.e.N......... .......PE..L...dx4`...........! ....&.....	success or wait	1	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\extndbrvvs.aly	unknown	16384	6b 07 ed c4 f8 ae be fb 22 29 33 ee e8 4e 66 9f 59 51 0e 65 df 9f a5 e7 fe 19 a2 c7 be c8 aa da 6c 16 df 2d a0 cd 55 97 63 e1 45 25 bc d7 6e 71 07 4f 93 ee d7 4f b3 6f 2c cd 65 66 0c 0c f0 7f 02 fd 4b b5 52 27 0a 6a 18 2c a5 98 49 28 b2 82 58 17 61 28 90 29 39 3b cf 63 bc eb 5d c6 4c ce 51 04 fc 1d 1f 62 ac fe ab 4f 72 fb bf 0e 9b 63 98 84 3e 7a 53 31 e1 22 52 94 36 c0 3f 40 67 0c 94 c9 29 82 6e 27 cd 7b 6f c5 1a da c3 9e c8 fb ec 80 05 ae 1c 1f de 81 c1 b9 9a cd 81 c6 62 09 f9 4c d7 7e 60 f9 45 77 01 c5 69 2d 1f 01 52 b3 4c f0 4d ec c7 3d 81 43 ce fe d6 51 c4 36 a6 53 65 ab 27 cb 68 c7 6f fa b5 20 49 a0 dd 61 b4 2b 1b f0 40 c6 08 ac 6d 33 fb bb 0b 96 8f e6 d2 b3 4d dd 20 97 8d a8 f4 96 78 3d 78 92 93 fb 7d cd 40 bf 10 36 fe d1 1c 6e 93 1b b9 12 3e f7 8a	k.......")3..Nf.YQ.e.......... ..l..- ..U.c.E%..nq.O...O.o,.ef ......K.R'.j.,..l(..X.a(.)9;.c ..].L.Q....b...Or....c..>zS1." R.6.?@g...).n'.{o............ ....b..L.~`.Ew..i-..R.L.M. .=.C...Q.6.Se.'.h.o.. I..a.+.. @...m3........M. .....x=x...}. @..6...n....>..	success or wait	18	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\nsmD8C8.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 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	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PAYMENT COPY.exe	unknown	512	success or wait	72	405E78	ReadFile
C:\Users\user\Desktop\PAYMENT COPY.exe	unknown	16384	success or wait	19	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsxD899.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsxD899.tmp	unknown	3510	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsxD899.tmp	unknown	4	success or wait	3	405E78	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\extndbrvvs.aly	unknown	279040	success or wait	1	72C34520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile

Analysis Process: PAYMENT COPY.exe PID: 6432 Parent PID: 6392

General

Start time:	08:11:49
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PAYMENT COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT COPY.exe'
Imagebase:	0x400000
File size:	332412 bytes
MD5 hash:	53E8C460446FE305DFC2159961AA6234
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: 00000001.00000002.498580778.0000000000599000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.498580778.0000000000599000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.498580778.0000000000599000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.500337236.0000000000730000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.500337236.0000000000730000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.499927530.00000000006C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.499927530.00000000006C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.500528462.0000000000780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.500528462.0000000000780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.505736368.000000000341C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.500087557.00000000006E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.500087557.00000000006E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000001.237862989.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000001.237862989.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000001.237862989.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.500417911.0000000000750000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.500417911.0000000000750000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.501309782.0000000002391000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.501562443.0000000002404000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.499796910.00000000006B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.499796910.00000000006B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.500251784.0000000000710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.500251784.0000000000710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.499394347.0000000000660000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.499394347.0000000000660000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.500213366.0000000000700000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.500213366.0000000000700000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.500144000.00000000006F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.500144000.00000000006F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.497023091.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.497023091.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.497023091.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.497023091.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.499506090.0000000000680000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.499506090.0000000000680000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.499715879.00000000006A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.499715879.00000000006A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.504422573.00000000027A5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.401079389.0000000003861000.00000004.00000001.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	6CE2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE2CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6BC7BEFF	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	6BC71E60	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	6BC7BEFF	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	6BC7DD66	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	6BC7DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEEDF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BC77038	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	6BC71E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF23B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BC77038	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	6BC7BEFF	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	6BC7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	11	6BC71E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BC71E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BC71E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEEDF.tmp	success or wait	1	6BC76A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpF23B.tmp	success or wait	1	6BC76A95	DeleteFileW
C:\Users\user\Desktop\PAYMENT COPY.exe:Zone.Identifier	success or wait	1	5258BA6	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	70 d8 ed bc 15 d8 d8 48	p.....H	success or wait	1	6BC71B4F	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 ad 31 29 81 e9 50 47 d2 e9 50 47 d2 e9 50 47 d2 2a 5f 18 d2 eb 50 47 d2 e9 50 46 d2 49 50 47 d2 2a 5f 1a d2 e6 50 47 d2 bd 73 77 d2 e3 50 47 d2 2e 56 41 d2 e8 50 47 d2 52 69 63 68 e9 50 47 d2 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5f d7 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 66 00 00 00 78 02 00 00 04 00 00 86 34 00 00 00 10 00 00 00 80 00 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1)..PG..PG..PG.*_... P G..PF.IPG.*_...PG..sw..PG ..VA. .PG.Rich.PG.........PE..L... _.$_.................f...x...... .4............@	success or wait	3	6BC7DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\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	6BC7DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEEDF.tmp	unknown	1306	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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6BC71B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	43	43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 44 65 73 6b 74 6f 70 5c 50 41 59 4d 45 4e 54 20 43 4f 50 59 2e 65 78 65	C:\Users\user\Desktop\PAYMENT COPY.exe	success or wait	1	6BC71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF23B.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	6BC71B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	4	6BC71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6BC71B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6BC71B4F	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	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CDED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CDED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6CDED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6CDED72F	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	6BC7646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 6532 Parent PID: 6432

General

Start time:	08:11:55
Start date:	23/02/2021
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\tmpEEDF.tmp'
Imagebase:	0xe90000
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\tmpEEDF.tmp	unknown	2	success or wait	1	E9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEEDF.tmp	unknown	1307	success or wait	1	E9ABD9	ReadFile

Analysis Process: conhost.exe PID: 6548 Parent PID: 6532

General

Start time:	08:11:55
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6596 Parent PID: 6432

General

Start time:	08:11:56
Start date:	23/02/2021
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\tmpF23B.tmp'
Imagebase:	0xe90000
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\tmpF23B.tmp	unknown	2	success or wait	1	E9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF23B.tmp	unknown	1311	success or wait	1	E9ABD9	ReadFile

Analysis Process: conhost.exe PID: 6604 Parent PID: 6596

General

Start time:	08:11:56
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PAYMENT COPY.exe PID: 6612 Parent PID: 1104

General

Start time:	08:11:56
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PAYMENT COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT COPY.exe' 0
Imagebase:	0x400000
File size:	332412 bytes
MD5 hash:	53E8C460446FE305DFC2159961AA6234
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: 00000007.00000002.264472405.0000000002A60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.264472405.0000000002A60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.264472405.0000000002A60000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.264472405.0000000002A60000.00000004.00000001.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~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsjF69F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user~1\AppData\Local\Temp\nsuF6DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	CreateDirectoryA
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsoF70E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	CreateDirectoryA
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsoF70E.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	405883	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsoF70E.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsjF69F.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsoF70E.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsuF6DF.tmp	unknown	22347	b6 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 f0 0c 00 00 01 00 00 00 b6 0d 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,...................$.	success or wait	19	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ri8clfcgml62un.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 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 f1 04 c3 1d b5 65 ad 4e b5 65 ad 4e b5 65 ad 4e b5 65 ac 4e 9f 65 ad 4e 49 12 14 4e ba 65 ad 4e 92 a3 63 4e b4 65 ad 4e 92 a3 67 4e b4 65 ad 4e 92 a3 64 4e b4 65 ad 4e 92 a3 61 4e b4 65 ad 4e 52 69 63 68 b5 65 ad 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 64 78 34 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 26 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $............e.N.e.N.e.N.e.N.e .NI..N.e.N..cN.e.N..gN.e.N. .dN .e.N..aN.e.NRich.e.N......... .......PE..L...dx4`...........! ....&.....	success or wait	1	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\extndbrvvs.aly	unknown	16384	6b 07 ed c4 f8 ae be fb 22 29 33 ee e8 4e 66 9f 59 51 0e 65 df 9f a5 e7 fe 19 a2 c7 be c8 aa da 6c 16 df 2d a0 cd 55 97 63 e1 45 25 bc d7 6e 71 07 4f 93 ee d7 4f b3 6f 2c cd 65 66 0c 0c f0 7f 02 fd 4b b5 52 27 0a 6a 18 2c a5 98 49 28 b2 82 58 17 61 28 90 29 39 3b cf 63 bc eb 5d c6 4c ce 51 04 fc 1d 1f 62 ac fe ab 4f 72 fb bf 0e 9b 63 98 84 3e 7a 53 31 e1 22 52 94 36 c0 3f 40 67 0c 94 c9 29 82 6e 27 cd 7b 6f c5 1a da c3 9e c8 fb ec 80 05 ae 1c 1f de 81 c1 b9 9a cd 81 c6 62 09 f9 4c d7 7e 60 f9 45 77 01 c5 69 2d 1f 01 52 b3 4c f0 4d ec c7 3d 81 43 ce fe d6 51 c4 36 a6 53 65 ab 27 cb 68 c7 6f fa b5 20 49 a0 dd 61 b4 2b 1b f0 40 c6 08 ac 6d 33 fb bb 0b 96 8f e6 d2 b3 4d dd 20 97 8d a8 f4 96 78 3d 78 92 93 fb 7d cd 40 bf 10 36 fe d1 1c 6e 93 1b b9 12 3e f7 8a	k......")3..Nf.YQ.e.......... ..l..- ..U.c.E%..nq.O...O.o,.ef ......K.R'.j.,..I(..X.a(.)9;.c ..].L.Q....b...Or....c..>zS1." R.6.?@g...).n'.{o............ ....b..L.~`.Ew..i-..R.L.M. .=.C...Q.6.Se.'.h.o.. I..a.+.. @...m3........M. .....x=x...}. @..6...n....>..	success or wait	18	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsoF70E.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 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	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PAYMENT COPY.exe	unknown	512	success or wait	72	405E78	ReadFile
C:\Users\user\Desktop\PAYMENT COPY.exe	unknown	16384	success or wait	19	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsuF6DF.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsuF6DF.tmp	unknown	3510	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsuF6DF.tmp	unknown	4	success or wait	3	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\extndbrvvs.aly	unknown	279040	success or wait	1	72C34520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile

Analysis Process: PAYMENT COPY.exe PID: 6712 Parent PID: 6612

General

Start time:	08:11:58
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PAYMENT COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT COPY.exe' 0
Imagebase:	0x400000
File size:	332412 bytes
MD5 hash:	53E8C460446FE305DFC2159961AA6234
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000008.00000002.278420831.0000000002460000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.278034704.00000000007CE000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.278034704.00000000007CE000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.278034704.00000000007CE000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.278506705.000000000344C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.278506705.000000000344C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.278355916.0000000002411000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.278466609.0000000003411000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.278466609.0000000003411000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.278466609.0000000003411000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.277405850.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.277405850.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.277405850.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.277405850.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.279255629.00000000049C2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.279255629.00000000049C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.279255629.00000000049C2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.279026119.00000000048F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.279026119.00000000048F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.279026119.00000000048F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.279026119.00000000048F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000001.257730823.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000001.257730823.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000001.257730823.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000001.257730823.0000000000400000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT COPY.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D13C78D	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\PAYMENT 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	6D13C907	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	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6744 Parent PID: 1104

General

Start time:	08:11:58
Start date:	23/02/2021
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:	332412 bytes
MD5 hash:	53E8C460446FE305DFC2159961AA6234
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsn15.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user~1\AppData\Local\Temp\nsn16.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	CreateDirectoryA
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsn15.tmp	success or wait	1	4036FD	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsn16.tmp	unknown	22347	b6 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 f0 0c 00 00 01 00 00 00 b6 0d 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....$.	success or wait	1	405EA7	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	72	405E78	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	16384	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsn16.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsn16.tmp	unknown	3510	success or wait	1	4032A5	ReadFile

Analysis Process: dhcpmon.exe PID: 5932 Parent PID: 3292

General

Start time:	08:12:07
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x400000
File size:	332412 bytes
MD5 hash:	53E8C460446FE305DFC2159961AA6234
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: 0000000E.00000002.286656662.0000000002A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.286656662.0000000002A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.286656662.0000000002A50000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.286656662.0000000002A50000.00000004.00000001.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~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsm24A4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user~1\AppData\Local\Temp\nsm24A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	CreateDirectoryA
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsc2504.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	CreateDirectoryA
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\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	4058C3	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsc2504.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	405883	CreateDirectoryA
C:\Users\user~1\AppData\Local\Temp\nsc2504.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsm24A4.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsc2504.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsm24A5.tmp	unknown	22347	b6 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 f0 0c 00 00 01 00 00 00 b6 0d 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,..................$.	success or wait	19	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ri8clfcgml62un.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 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 f1 04 c3 1d b5 65 ad 4e b5 65 ad 4e b5 65 ad 4e b5 65 ac 4e 9f 65 ad 4e 49 12 14 4e ba 65 ad 4e 92 a3 63 4e b4 65 ad 4e 92 a3 67 4e b4 65 ad 4e 92 a3 64 4e b4 65 ad 4e 92 a3 61 4e b4 65 ad 4e 52 69 63 68 b5 65 ad 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 64 78 34 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 26 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $............e.N.e.N.e.N.e.N.e .NI..N.e.N..cN.e.N..gN.e.N. .dN .e.N..aN.e.NRich.e.N......... .......PE..L...dx4`...........! ....&.....	success or wait	1	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\extndbrvvs.aly	unknown	16384	6b 07 ed c4 f8 ae be fb 22 29 33 ee e8 4e 66 9f 59 51 0e 65 df 9f a5 e7 fe 19 a2 c7 be c8 aa da 6c 16 df 2d a0 cd 55 97 63 e1 45 25 bc d7 6e 71 07 4f 93 ee d7 4f b3 6f 2c cd 65 66 0c 0c f0 7f 02 fd 4b b5 52 27 0a 6a 18 2c a5 98 49 28 b2 82 58 17 61 28 90 29 39 3b cf 63 bc eb 5d c6 4c ce 51 04 fc 1d 1f 62 ac fe ab 4f 72 fb bf 0e 9b 63 98 84 3e 7a 53 31 e1 22 52 94 36 c0 3f 40 67 0c 94 c9 29 82 6e 27 cd 7b 6f c5 1a da c3 9e c8 fb ec 80 05 ae 1c 1f de 81 c1 b9 9a cd 81 c6 62 09 f9 4c d7 7e 60 f9 45 77 01 c5 69 2d 1f 01 52 b3 4c f0 4d ec c7 3d 81 43 ce fe d6 51 c4 36 a6 53 65 ab 27 cb 68 c7 6f fa b5 20 49 a0 dd 61 b4 2b 1b f0 40 c6 08 ac 6d 33 fb bb 0b 96 8f e6 d2 b3 4d dd 20 97 8d a8 f4 96 78 3d 78 92 93 fb 7d cd 40 bf 10 36 fe d1 1c 6e 93 1b b9 12 3e f7 8a	k.......")3..Nf.YQ.e.......... ..l..- ..U.c.E%..nq.O...O.o,.ef ......K.R'.j.,..I(..X.a(.)9;.c ..].L.Q....b...Or....c..>zS1." R.6.?@g...).n'.{o............ ....b..L.~`.Ew..i-..R.L.M. .=.C...Q.6.Se.'.h.o.. I..a.+.. @...m3........M. .....x=x...}. @..6...n....>..	success or wait	18	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc2504.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 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	405EA7	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	72	405E78	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	16384	success or wait	19	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsm24A5.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsm24A5.tmp	unknown	3510	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsm24A5.tmp	unknown	4	success or wait	3	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\extndbrvvs.aly	unknown	279040	success or wait	1	72C34520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	72C3387B	ReadFile

Analysis Process: dhcpmon.exe PID: 2896 Parent PID: 5932

General

Start time:	08:12:09
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x400000
File size:	332412 bytes
MD5 hash:	53E8C460446FE305DFC2159961AA6234
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.298632979.00000000022E0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.298228465.000000000054A000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.298228465.000000000054A000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.298228465.000000000054A000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.298702640.00000000032CC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.298702640.00000000032CC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.298677896.0000000003291000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.298677896.0000000003291000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.298677896.0000000003291000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.298074708.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.298074708.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.298074708.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.298074708.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.299582604.00000000047B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.299582604.00000000047B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.299582604.00000000047B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.299582604.00000000047B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.300040048.0000000004E32000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.300040048.0000000004E32000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.300040048.0000000004E32000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000001.281117600.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000001.281117600.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000001.281117600.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.298587099.0000000002291000.00000004.00000001.sdmp, Author: Joe Security
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	6CE2CF06	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	6CE2CF06	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	6D13C78D	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	6D13C907	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	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile

Disassembly

Code Analysis