ID: 711673
Sample Name: attached PI.exe
Cookbook: default.jbs
Time: 12:03:48
Date: 28/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

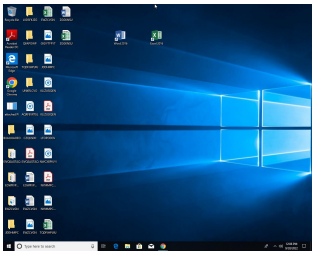
Windows Analysis Report

attached PI.exe

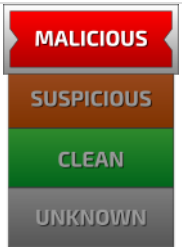
Overview

General Information

Sample Name:	attached PI.exe
Analysis ID:	711673
MD5:	238b41e834f3b6..
SHA1:	006efa65c3a4c5...
SHA256:	e0b3c7281dd348..
Infos:	



Detection



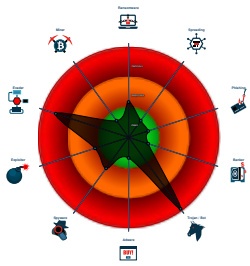
Nanocore

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

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- Multi AV Scanner detection for drop...
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other...

Classification



Process Tree

- **System is w10x64**
- attached PI.exe (PID: 1604 cmdline: "C:\Users\user\Desktop\attached PI.exe" MD5: 238B41E834F3B663584D4788493BC75F)
  - schtasks.exe (PID: 3836 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmpE760.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - attached PI.exe (PID: 3092 cmdline: {path} MD5: 238B41E834F3B663584D4788493BC75F)
  - attached PI.exe (PID: 4748 cmdline: {path} MD5: 238B41E834F3B663584D4788493BC75F)
    - schtasks.exe (PID: 4648 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpD63A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5328 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmpD9B5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- attached PI.exe (PID: 5344 cmdline: "C:\Users\user\Desktop\attached PI.exe" 0 MD5: 238B41E834F3B663584D4788493BC75F)
  - schtasks.exe (PID: 5072 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmp6181.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - attached PI.exe (PID: 5216 cmdline: {path} MD5: 238B41E834F3B663584D4788493BC75F)
  - attached PI.exe (PID: 2192 cmdline: {path} MD5: 238B41E834F3B663584D4788493BC75F)
- dhcpmon.exe (PID: 4596 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 238B41E834F3B663584D4788493BC75F)
  - schtasks.exe (PID: 6132 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmp6CEB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 4460 cmdline: {path} MD5: 238B41E834F3B663584D4788493BC75F)
- dhcpmon.exe (PID: 4812 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 238B41E834F3B663584D4788493BC75F)
  - schtasks.exe (PID: 5920 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmp8C89.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5184 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 2620 cmdline: {path} MD5: 238B41E834F3B663584D4788493BC75F)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "fba1bbc6-2cc8-4c94-b6c0-dda5a12f",
  "Group": "Default",
  "Domain1": "brightnano1.ddns.net",
  "Domain2": "",
  "Port": 1989,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x16e3:$x2: NanoCore.ClientPluginHost • 0x1800:$s4: PipeCreated • 0x16fd:$s5: IClientLoggingHost
0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x175f:$x2: NanoCore.ClientPlugin • 0x16e3:$x3: NanoCore.ClientPluginHost • 0x1775:$i3: IClientNetwork • 0x16fd:$i6: IClientLoggingHost • 0x171c:$i7: IClientNetworkHost • 0x1491:$s1: ClientPlugin • 0x1768:$s1: ClientPlugin
0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x16e3:$a1: NanoCore.ClientPluginHost • 0x175f:$a2: NanoCore.ClientPlugin • 0x16fd:$b9: IClientLoggingHost
0000000A.00000002.574582318.0000000003E61000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x27b0b:$a1: NanoCore.ClientPluginHost • 0x27ae2:$a2: NanoCore.ClientPlugin • 0x2cb36:$b7: LogClientException • 0x27af8:$b9: IClientLoggingHost

Click to see the 105 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.attached PI.exe.7280000.26.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
10.2.attached Pl.exe.7280000.26.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
10.2.attached Pl.exe.7280000.26.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x5ad5:$x2: NanoCore.ClientPlugin • 0x59eb:$x3: NanoCore.ClientPluginHost • 0x5aeb:$i3: IClientNetwork • 0x5a24:$i5: IClientDataHost • 0x5a05:$i6: IClientLoggingHost • 0x5b48:$i7: IClientNetworkHost • 0x5a43:$i8: IClientUIHost • 0x6955:$i9: IClientNameObjectCollection • 0x54fc:$s1: ClientPlugin • 0x5ade:$s1: ClientPlugin • 0x6971:$s6: get_ClientSettings
10.2.attached Pl.exe.7280000.26.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x59eb:$a1: NanoCore.ClientPluginHost • 0x5ad5:$a2: NanoCore.ClientPlugin • 0x732e:$b7: LogClientException • 0x6941:$b8: PipeExists • 0x5a05:$b9: IClientLoggingHost
10.2.attached Pl.exe.40c4695.11.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x3bd6:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
Click to see the 268 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170 −

Timestamp:	192.168.2.4171.22.30.170497011989281676 6 09/28/22-12:05:02.686443
SID:	2816766
Source Port:	49701
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170 −

Timestamp:	192.168.2.4171.22.30.170497031989202501 9 09/28/22-12:05:22.049360

SID:	2025019
Source Port:	49703
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.1704970819892816766 09/28/22-12:06:01.338770
SID:	2816766
Source Port:	49708
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.1704971119892816766 09/28/22-12:06:22.172077
SID:	2816766
Source Port:	49711
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.1704970719892025019 09/28/22-12:05:54.025166
SID:	2025019
Source Port:	49707
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.1704971319892025019 09/28/22-12:06:32.627748
SID:	2025019
Source Port:	49713
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.1704970619892816718 09/28/22-12:05:48.890995
SID:	2816718
Source Port:	49706
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.1704970919892025019 09/28/22-12:06:06.469048
SID:	2025019
Source Port:	49709
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.1704971019892816766 09/28/22-12:06:14.491368
SID:	2816766
Source Port:	49710
Destination Port:	1989
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970419892025019 09/28/22-12:05:33.183062
SID:	2025019
Source Port:	49704
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970419892816766 09/28/22-12:05:33.986316
SID:	2816766
Source Port:	49704
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704971019892025019 09/28/22-12:06:13.098552
SID:	2025019
Source Port:	49710
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704971319892816766 09/28/22-12:06:34.136588
SID:	2816766
Source Port:	49713
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704971419892025019 09/28/22-12:06:40.121067
SID:	2025019
Source Port:	49714
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 171.22.30.170 - Destination IP: 192.168.2.4	
Timestamp:	171.22.30.170192.168.2.41989497142841753 09/28/22-12:07:00.176130
SID:	2841753
Source Port:	1989
Destination Port:	49714
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970819892025019 09/28/22-12:06:00.252868
SID:	2025019
Source Port:	49708
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704971119892025019 09/28/22-12:06:19.288235

SID:	2025019
Source Port:	49711
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.170497061989281676 6 09/28/22-12:05:48.890995
SID:	2816766
Source Port:	49706
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.170497011989202501 9 09/28/22-12:05:00.703490
SID:	2025019
Source Port:	49701
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.170497031989281676 6 09/28/22-12:05:23.115950
SID:	2816766
Source Port:	49703
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 171.22.30.170 - Destination IP: 192.168.2.4	−
Timestamp:	171.22.30.170192.168.2.41989497052810290 09/28/22-12:05:40.491149
SID:	2810290
Source Port:	1989
Destination Port:	49705
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.170497051989202501 9 09/28/22-12:05:40.016972
SID:	2025019
Source Port:	49705
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.170497121989202501 9 09/28/22-12:06:26.713238
SID:	2025019
Source Port:	49712
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	−
Timestamp:	192.168.2.4171.22.30.170497121989281676 6 09/28/22-12:06:27.481705
SID:	2816766
Source Port:	49712
Destination Port:	1989
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970219892025019 09/28/22-12:05:11.687415
SID:	2025019
Source Port:	49702
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970219892816766 09/28/22-12:05:12.780673
SID:	2816766
Source Port:	49702
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970519892816766 09/28/22-12:05:41.772448
SID:	2816766
Source Port:	49705
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970619892025019 09/28/22-12:05:47.986712
SID:	2025019
Source Port:	49706
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 171.22.30.170	
Timestamp:	192.168.2.4171.22.30.1704970919892816766 09/28/22-12:06:07.869293
SID:	2816766
Source Port:	49709
Destination Port:	1989
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

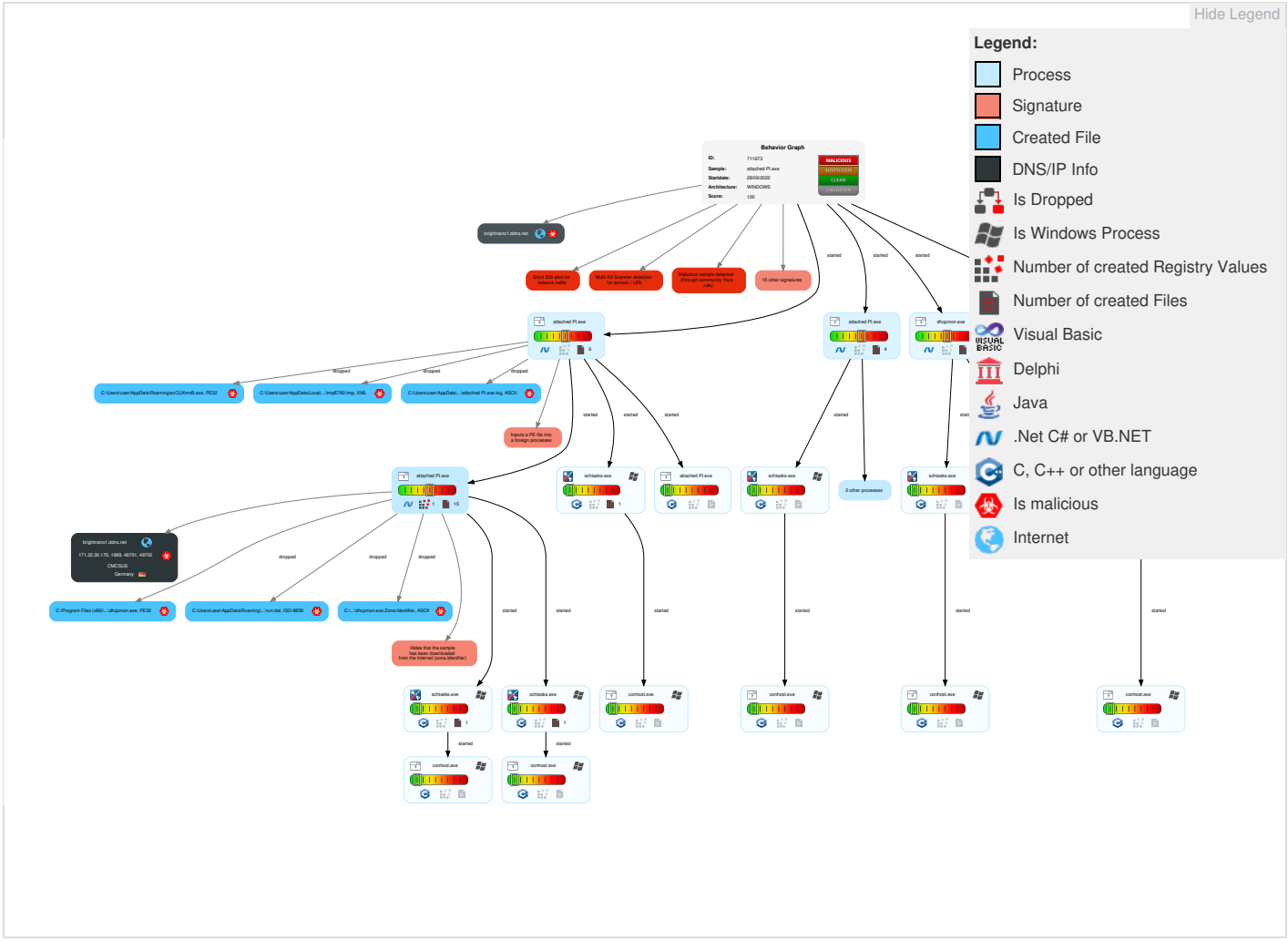
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	1 1 Input Capture	2 1 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

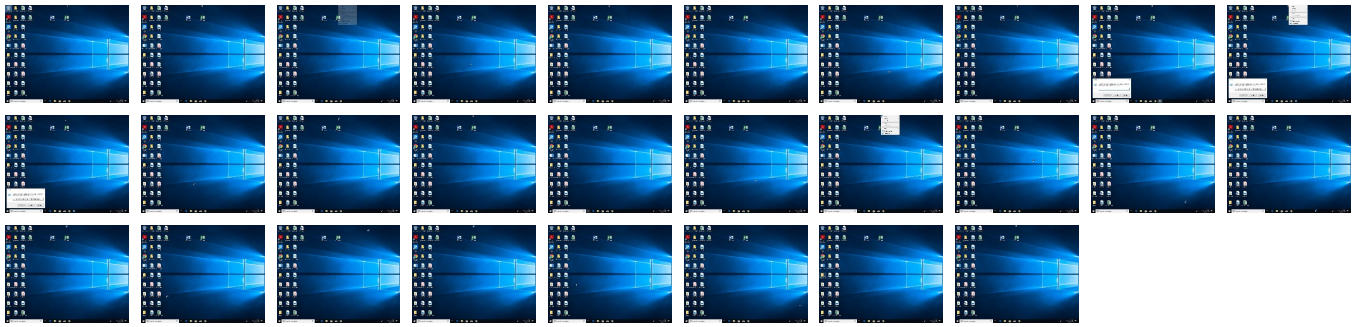
Behavior Graph



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
attached PI.exe	28%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
attached PI.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ecCUXmnB.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	28%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Roaming\ecCUXmnB.exe	28%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.attached PI.exe.59a0000.18.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.attached PI.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
brightnano1.ddns.net	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fonts.comn-u	0%	URL Reputation	safe	
http://www.urwpp.deF	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comF2muP	0%	Avira URL Cloud	safe	
	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals)m	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krendDo;P	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://en.wl	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaen	0%	Avira URL Cloud	safe	
http://www.fontbureau.comnn	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFVm)P	0%	Avira URL Cloud	safe	
http://www.tiro.comn7OgPF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtoed	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krntaD/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comTTFd_m	0%	Avira URL Cloud	safe	
http://www.fontbureau.comL.TTF;mzP	0%	Avira URL Cloud	safe	
http://www.fonts.com(O	0%	Avira URL Cloud	safe	
http://www.tiro.comSO	0%	Avira URL Cloud	safe	
brightnano1.ddns.net	100%	Avira URL Cloud	malware	
http://www.sajatypeworks.comn-uX0	0%	Avira URL Cloud	safe	
http://www.fonts.come	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiefMm	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/-	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
brightnano1.ddns.net	171.22.30.170	true	true	• 14%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
brightnano1.ddns.net	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

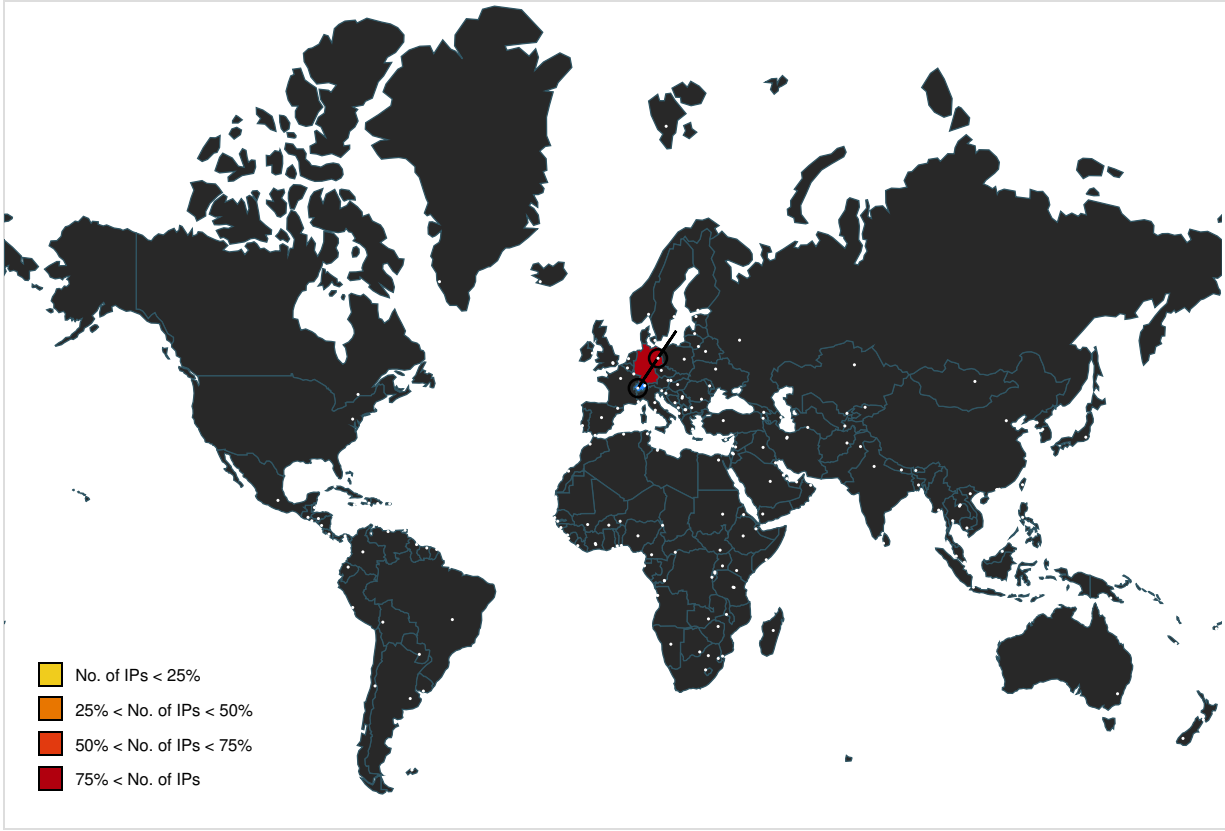
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF2muP	attached PI.exe, 00000003.00000003.29733 4590.0000000005F4A000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.297020606.0000000005F 49000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://en.wl	attached PI.exe, 00000003.00000003.28966 2678.000000000160D000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krendDo;P	attached PI.exe, 00000003.00000003.29189 5691.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comals)m	attached PI.exe, 00000003.00000003.29799 1182.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers?	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.comaen	attached PI.exe, 00000003.00000003.32565 3593.0000000005F40000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290734249.0000000005F 5B000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comnn	attached PI.exe, 00000003.00000003.29702 0606.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.comtoed	attached PI.exe, 00000003.00000003.29702 0606.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	attached PI.exe, 0000000A.00000002.57591 7734.0000000003FE2000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 0000000A.00000002.563358454.0000000002E A9000.00000004.00000800.00020000.0000000 0.sdmp, attached PI.exe, 0000000A.000000 02.578123416.000000000414E000.00000004.0 0000800.00020000.00000000.sdmp, attached PI.exe, 0000000A.00000002.588382533.0000000007280 000.00000004.08000000.00040000.00000000.sdmp, attached PI.exe, 0000000A.00000002.577106409 .00000000040AA000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.fontbureau.comFVm)P	attached PI.exe, 00000003.00000003.29799 1182.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	attached PI.exe, 00000003.00000003.28995 8917.0000000005F5B000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000002.338387946.00000000071 52000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comn7OgPF	attached PI.exe, 00000003.00000003.29075 4999.0000000005F5B000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krntaD/	attached PI.exe, 00000003.00000003.29189 5691.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comTTFd_m	attached PI.exe, 00000003.00000003.29799 1182.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comL.TTF;mzP	attached PI.exe, 00000003.00000003.29733 4590.0000000005F4A000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.297020606.0000000005F 49000.00000004.00000800.00020000.0000000 0.sdmp, attached PI.exe, 00000003.000000 03.297991182.0000000005F49000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/	attached PI.exe, 00000003.00000003.29702 0606.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.296598172.0000000005F 48000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.galapagosdesign.com/DPlease	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	attached PI.exe, 00000003.00000003.29024 9380.0000000005F64000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290309072.0000000005F 64000.00000004.00000800.00020000.0000000 0.sdmp, attached PI.exe, 00000003.000000 03.290425292.0000000005F5B000.00000004.0 0000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000002.338387946.0000000007152 000.00000004.00000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290289127 .0000000005F5B000.00000004.00000800.0002 0000.00000000.sdmp, attached PI.exe, 000 00003.00000003.290232356.0000000005F5B00 0.00000004.00000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290377873.0 000000005F5B000.00000004.00000800.000200 00.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	attached PI.exe, 00000003.00000003.29189 5691.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000002.338387946.00000000071 52000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	attached PI.exe, 00000003.00000003.29799 1182.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	attached PI.exe, 00000003.00000002.32807 5400.0000000002F51000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 0000000A.00000002.563358454.0000000002E A9000.00000004.00000800.00020000.0000000 0.sdmp, attached PI.exe, 0000000F.000000 02.403498358.0000000002F3D000.00000004.0 0000800.00020000.00000000.sdmp, dhcpmon.exe, 00000010.00000002.409484512.0000000002CD1000. 00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000011.00000002.4315729 00.000000000281D000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fonts.com(O	attached PI.exe, 00000003.00000003.29028 9127.0000000005F5B000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sakkal.com	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comSO	attached PI.exe, 00000003.00000003.29075 4999.0000000005F5B000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com	attached PI.exe, 00000003.00000003.29799 1182.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000002.338387946.00000000071 52000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.fontbureau.comF	attached PI.exe, 00000003.00000003.29702 0606.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.come	attached PI.exe, 00000003.00000003.29030 9072.0000000005F64000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn-u	attached PI.exe, 00000003.00000003.29024 9380.0000000005F64000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290309072.0000000005F 64000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comn-uX0	attached PI.exe, 00000003.00000003.29000 1259.0000000005F63000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290249380.0000000005F 64000.00000004.00000800.00020000.0000000 0.sdmp, attached PI.exe, 00000003.000000 03.290309072.0000000005F64000.00000004.0 0000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290366189.0000000005F64 000.00000004.00000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290043716 .0000000005F64000.00000004.00000800.0002 0000.00000000.sdmp, attached PI.exe, 000 00003.00000003.290206189.0000000005F6400 0.00000004.00000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.289958917.0 000000005F5B000.00000004.00000800.000200 00.00000000.sdmp, attached PI.exe, 00000 003.00000003.290142745.0000000005F64000. 00000004.00000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.290177451.000 0000005F64000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deF	attached PI.exe, 00000003.00000003.29659 8172.0000000005F48000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	attached PI.exe, 00000003.00000003.29702 0606.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.297991182.0000000005F 49000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	attached PI.exe, 00000003.00000003.29334 5954.0000000005F44000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	attached PI.exe, 00000003.00000003.29283 8602.0000000005F7D000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.293361358.0000000005F 49000.00000004.00000800.00020000.0000000 0.sdmp, attached PI.exe, 00000003.000000 03.292992929.0000000005F44000.00000004.0 0000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000002.338387946.0000000007152 000.00000004.00000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.293345954 .0000000005F44000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.comsiefMm	attached PI.exe, 00000003.00000003.29799 1182.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	attached PI.exe, 00000003.00000003.29743 4096.0000000005F7D000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.297581397.0000000005F 7D000.00000004.00000800.00020000.0000000 0.sdmp, attached PI.exe, 00000003.000000 03.297534861.0000000005F7D000.00000004.0 0000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.297508471.0000000005F7D 000.00000004.00000800.00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.297455091 .0000000005F7D000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	attached PI.exe, 00000003.00000003.32565 3593.0000000005F40000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	attached PI.exe, 00000003.00000002.33838 7946.0000000007152000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com/deDn:Pg	attached PI.exe, 00000003.00000003.29733 4590.0000000005F4A000.00000004.00000800. 00020000.00000000.sdmp, attached PI.exe, 00000003.00000003.297020606.0000000005F 49000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.fontbureau.comals	attached PI.exe, 00000003.00000003.29799 1182.0000000005F49000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/-	attached PI.exe, 00000003.00000003.29334 5954.0000000005F44000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
171.22.30.170	brightnano1.ddns.net	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	711673
Start date and time:	2022-09-28 12:03:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	attached PI.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
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@34/16@14/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:04:44	API Interceptor	828x Sleep call for process: attached PI.exe modified
12:04:55	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
12:04:56	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\attached PI.exe" s>$(Arg0)
12:04:58	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
12:05:17	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1131520
Entropy (8bit):	6.901099612044746
Encrypted:	false

SSDEEP:	12288:c3mY2iNw0+9MKvADqjJ5nr9fAn/CoE2g++sn3Qwon89AGPEAbVNqPKvmvuoZ2aVc:c3x1leyjrrm/C72g2QFnE7P5
MD5:	238B41E834F3B663584D4788493BC75F
SHA1:	006EFA65C3A4C5B4EE2402AB5E6D789FC95E0B9C
SHA-256:	E0B3C7281DD3488DF3C71EE35DDE8FE321E5AAE4D3F200D2F63DFEF64A97DAFF
SHA-512:	23A862D13B143D37328E8055D99329E0EC5CAAA0A554706EB18AD3E0AC298BB5E10141F9101019223BFE77F2ABCADFE90E27B91A453C5CF6CB8FE37396AF956D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ....@.....\...O.....8..... ....H.....text..... ....`.rsrc...8.....@..@.reloc..... .....B.....@..B.....H.....V.....8.....*..($...*&..(%....*.s&.....s'.....s(.....s).....s*.....*Z.....o=.....*&..(>....*j..{....(...+} .....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(.. .+}.....{....+.*...{.....,.+.....,.rq..ps@...z..

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

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\attached PI.exe.log

Process:	C:\Users\user\Desktop\attached PI.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:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8F8
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp6181.tmp

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.178198085945928
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGFtn:cbhK79lNQR/rydbz9I3YODOLNdq30
MD5:	D44529740ECFF6AE70C76D0A3C410D4C
SHA1:	4F89B46804F9DD3C912F1339E67A47F17CC71889
SHA-256:	A53275C1E247E1D887956DBDE3C9CA1AAA72269BD65D9A2A2D4F31CF36D67491
SHA-512:	41B22B3AE8679A5ECCCD084D2194FB611F6D3FF040FED381DE0AF3FA1DAF339A7B44E94180F2AC7FB63F106CF199135B9C4EA0FFA848CEB5024CDEB9881546 60
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp6CEB.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.178198085945928
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGFtn:cbhK79lNQR/rydbz9I3YODOLNdq30
MD5:	D44529740ECFF6AE70C76D0A3C410D4C
SHA1:	4F89B46804F9DD3C912F1339E67A47F17CC71889
SHA-256:	A53275C1E247E1D887956DBDE3C9CA1AAA72269BD65D9A2A2D4F31CF36D67491
SHA-512:	41B22B3AE8679A5ECCCD084D2194FB611F6D3FF040FED381DE0AF3FA1DAF339A7B44E94180F2AC7FB63F106CF199135B9C4EA0FFA848CEB5024CDEB9881546 60
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp8C89.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.178198085945928
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGFtn:cbhK79lNQR/rydbz9I3YODOLNdq30
MD5:	D44529740ECFF6AE70C76D0A3C410D4C
SHA1:	4F89B46804F9DD3C912F1339E67A47F17CC71889
SHA-256:	A53275C1E247E1D887956DBDE3C9CA1AAA72269BD65D9A2A2D4F31CF36D67491

SHA-512:	41B22B3AE8679A5ECCCD084D2194FB611F6D3FF040FED381DE0AF3FA1DAF339A7B44E94180F2AC7FB63F106CF199135B9C4EA0FFA848CEB5024CDEB988154660
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpD63A.tmp

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.091259752872306
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Yc1xtn:cbk4oL600QydbQxIYODOLedq3I1j
MD5:	05CB9D147938E4D615808C78EC195503
SHA1:	CEC5B9AF5ADCE5DF733B630917C2FA999C806019
SHA-256:	7D3AB0C2A42695005C8E1B42350AE0DDB7376F3CA12F2E4DDA3701FE53AB8FD6
SHA-512:	D9349D1146E4E65C06BE6E60D66DE4E49A0AFD312EC468E6D4EFBFEB5AF92E265B4A445ECD31E81975546C5A6FEC91F0CD6B35548805B5068BB8409A10B98FC4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpD9B5.tmp

Process:	C:\Users\user\Desktop\attached PI.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:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpE760.tmp

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.178198085945928
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGFtn:cbhK79lNQR/rydbz9I3YODOLNdq30
MD5:	D44529740ECFF6AE70C76D0A3C410D4C
SHA1:	4F89B46804F9DD3C912F1339E67A47F17CC71889
SHA-256:	A53275C1E247E1D887956DBDE3C9CA1AAA72269BD65D9A2A2D4F31CF36D67491

SHA-512:	41B22B3AE8679A5ECCCD084D2194FB611F6D3FF040FED381DE0AF3FA1DAF339A7B44E94180F2AC7FB63F106CF199135B9C4EA0FFA848CEB5024CDEB988154660
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

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

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Dq:e
MD5:	6A2D94F5982D067BF2A1AB36640A7E5E
SHA1:	6F5ABF73D95734947FF9C95EBC4F8F58665D8B31
SHA-256:	0D0B21D2A7CE3DB3F754897DBF994F8C0F04BD005D5F013143450F1DB032E41E
SHA-512:	7022B33CE54E134E018FF88F5B683751FBD0146E0AAB4B24E872FE998FB46A7FE6076ED09C240520EB93D64B5E78726A7E4D72156B3822090A677BBBFDE19C0C
Malicious:	**true**
Preview:	.S..8..H

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

Process:	C:\Users\user\Desktop\attached PI.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:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
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\attached PI.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:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV.,,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.............b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.........$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

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

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.188331131693838
Encrypted:	false
SSDEEP:	3:oNt+WfWE05C:oNwvEEC
MD5:	AF41AEE5DDE3AEBD95B39C61F92F2814
SHA1:	B513EE3B2578182B7AA3A0AB5D71B4698A2B82F2
SHA-256:	C4E0DFFF3F4206C47C3D8893BADA97A68D5236D75ADE3947D5B09A2D8C0F2D00
SHA-512:	24D9C0BE8BD4B95E34B7FE87715D531925DEFFE2B87739BF8F6132B1C3C59070C35853F44A58974E67FFD84BBF40AB2B99BFDD29FEB54B102596F715F3335AFD
Malicious:	false
Preview:	C:\Users\user\Desktop\attached PI.exe

C:\Users\user\AppData\Roaming\ecCUXmnB.exe

Process:	C:\Users\user\Desktop\attached PI.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1131520
Entropy (8bit):	6.901099612044746
Encrypted:	false
SSDEEP:	12288:c3mY2iNw0+9MKvADqjJ5nr9fAn/CoE2g++sn3Qwon89AGPEAbVNqPKvmvuoZ2aVc:c3x1leyjrrm/C72g2QFnE7P5
MD5:	238B41E834F3B663584D4788493BC75F
SHA1:	006EFA65C3A4C5B4EE2402AB5E6D789FC95E0B9C
SHA-256:	E0B3C7281DD3488DF3C71EE35DDE8FE321E5AAE4D3F200D2F63DFEF64A97DAFF
SHA-512:	23A862D13B143D37328E8055D99329E0EC5CAAA0A554706EB18AD3E0AC298BB5E10141F9101019223BFE77F2ABCADFE90E27B91A453C5CF6CB8FE37396AF956D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ..@.....\...O.....8..... .....H.....text..... .....`.rsrc...8.....@..@.reloc.....B.....@..B.....H.....V.....8.....*..($...*&..(%....*.s&.....s'.....s(.....s).....s*.....*Z.....o=.....*&..(>....*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*...{.....,.+.....,.rq..ps@...z..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Entropy (8bit):	6.901099612044746
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	attached PI.exe
File size:	1131520
MD5:	238b41e834f3b663584d4788493bc75f
SHA1:	006efa65c3a4c5b4ee2402ab5e6d789fc95e0b9c
SHA256:	e0b3c7281dd3488df3c71ee35dde8fe321e5aae4d3f200d2f63dfef64a97daff
SHA512:	23a862d13b143d37328e8055d99329e0ec5caaa0a554706eb18ad3e0ac298bb5e10141f9101019223bfe77f2abcadfe90e27b91a453c5cf6cb8fe37396af956d
SSDEEP:	12288:c3mY2iNw0+9MKvADqjJ5nr9fAn/CoE2g++sn3Qwon89AGPEAbVNqPKvmvuoZ2aVc:c3x1leyjrrm/C72g2QFnE7P5
TLSH:	4B353B1432E676BDF07787B65FC4BCF99B96F936431A90B224A72349472AD02CDE1072
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. .....@.....

File Icon

Icon Hash:	009abababababa00

Static PE Info

General

Entrypoint:	0x50a5ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xA0F4C794 [Wed Jul 28 14:07:16 2055 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10a55c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10c000	0xb838	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x118000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1085b4	0x108600	False	0.6172909278959811	data	6.975603145945541	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0xb838	0xba00	False	0.09587113575268817	data	3.6981687259727196	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x118000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10c280	0x8b3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10cb34	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 0		
RT_ICON	0x110d5c	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x113304	0x1a68	Device independent bitmap graphic, 40 x 80 x 32, image size 0		
RT_ICON	0x114d6c	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x115e14	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x11679c	0x6b8	Device independent bitmap graphic, 20 x 40 x 32, image size 0		
RT_ICON	0x116e54	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_GROUP_ICON	0x1172bc	0x76	data		
RT_VERSION	0x117334	0x314	data		
RT_MANIFEST	0x117648	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

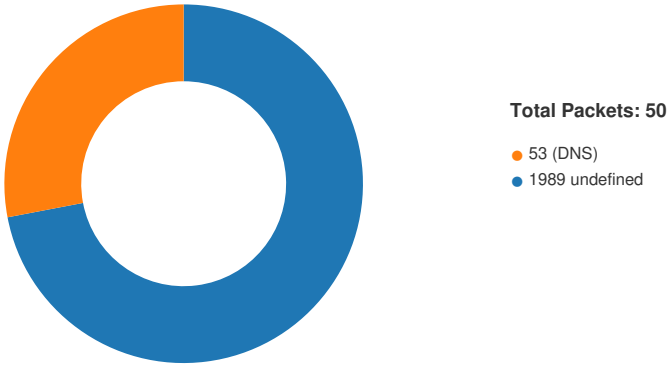
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4171.22.30.1704970119892816766 09/28/22-12:05:02.686443	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970319892025019 09/28/22-12:05:22.049360	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970819892816766 09/28/22-12:06:01.338770	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971119892816766 09/28/22-12:06:22.172077	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970719892025019 09/28/22-12:05:54.025166	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971319892025019 09/28/22-12:06:32.627748	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970619892816718 09/28/22-12:05:48.890995	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49706	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970919892025019 09/28/22-12:06:06.469048	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971019892816766 09/28/22-12:06:14.491368	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970419892025019 09/28/22-12:05:33.183062	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	1989	192.168.2.4	171.22.30.170

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4171.22.30.1704970419892816766 09/28/22-12:05:33.986316	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971019892025019 09/28/22-12:06:13.098552	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971319892816766 09/28/22-12:06:34.136588	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971419892025019 09/28/22-12:06:40.121067	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	1989	192.168.2.4	171.22.30.170
171.22.30.170192.168.2.41989497142841753 09/28/22-12:07:00.176130	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1989	49714	171.22.30.170	192.168.2.4
192.168.2.4171.22.30.1704970819892025019 09/28/22-12:06:00.252868	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971119892025019 09/28/22-12:06:19.288235	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970619892816766 09/28/22-12:05:48.890995	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970119892025019 09/28/22-12:05:00.703490	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970319892816766 09/28/22-12:05:23.115950	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	1989	192.168.2.4	171.22.30.170
171.22.30.170192.168.2.41989497052810290 09/28/22-12:05:40.491149	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1989	49705	171.22.30.170	192.168.2.4
192.168.2.4171.22.30.1704970519892025019 09/28/22-12:05:40.016972	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971219892025019 09/28/22-12:06:26.713238	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704971219892816766 09/28/22-12:06:27.481705	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970219892025019 09/28/22-12:05:11.687415	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970219892816766 09/28/22-12:05:12.780673	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970519892816766 09/28/22-12:05:41.772448	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970619892025019 09/28/22-12:05:47.986712	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	1989	192.168.2.4	171.22.30.170
192.168.2.4171.22.30.1704970919892816766 09/28/22-12:06:07.869293	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	1989	192.168.2.4	171.22.30.170

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 12:05:00.422650099 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:00.450193882 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:00.450310946 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:00.703490019 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:00.785625935 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:00.810659885 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:00.859870911 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:00.888756037 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.052102089 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.407006025 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.487763882 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.487885952 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.557956934 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.557982922 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.558001995 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.558022022 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.558062077 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.558096886 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.585247993 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585284948 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585310936 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585339069 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.585357904 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585383892 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585410118 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585421085 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.585443020 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.585455894 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585481882 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.585517883 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612560987 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612585068 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612601995 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612620115 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612639904 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612654924 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612665892 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612679005 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612694979 CEST	1989	49701	171.22.30.170	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 12:05:01.612710953 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612730980 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612735987 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612751007 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612759113 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612775087 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612787008 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612797976 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612812996 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612829924 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612845898 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612853050 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.612865925 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.612876892 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.613022089 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640002966 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640031099 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640053034 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640075922 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640089989 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640117884 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640127897 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640150070 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640172005 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640192986 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640212059 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640223980 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640233994 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640254021 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640274048 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640295029 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640306950 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640327930 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640335083 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640356064 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640377045 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640398026 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640410900 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640429974 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640439987 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640460014 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640480995 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640497923 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640511036 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640531063 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640551090 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640575886 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640593052 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640594006 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640635967 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640656948 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640681028 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640692949 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640712976 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640722036 CEST	49701	1989	192.168.2.4	171.22.30.170
Sep 28, 2022 12:05:01.640741110 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640762091 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640783072 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640804052 CEST	49701	1989	192.168.2.4	171.22.30.170

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 12:05:01.640813112 CEST	1989	49701	171.22.30.170	192.168.2.4
Sep 28, 2022 12:05:01.640824080 CEST	49701	1989	192.168.2.4	171.22.30.170

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 28, 2022 12:05:00.383311987 CEST	59683	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:05:00.403003931 CEST	53	59683	8.8.8.8	192.168.2.4
Sep 28, 2022 12:05:11.635108948 CEST	64167	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:05:11.654015064 CEST	53	64167	8.8.8.8	192.168.2.4
Sep 28, 2022 12:05:21.996689081 CEST	58565	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:05:22.016352892 CEST	53	58565	8.8.8.8	192.168.2.4
Sep 28, 2022 12:05:32.530100107 CEST	52239	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:05:32.551434040 CEST	53	52239	8.8.8.8	192.168.2.4
Sep 28, 2022 12:05:39.939918041 CEST	56807	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:05:39.963004112 CEST	53	56807	8.8.8.8	192.168.2.4
Sep 28, 2022 12:05:47.937693119 CEST	61007	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:05:47.957211018 CEST	53	61007	8.8.8.8	192.168.2.4
Sep 28, 2022 12:05:53.971554041 CEST	60686	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:05:53.992727041 CEST	53	60686	8.8.8.8	192.168.2.4
Sep 28, 2022 12:06:00.200548887 CEST	61124	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:06:00.220154047 CEST	53	61124	8.8.8.8	192.168.2.4
Sep 28, 2022 12:06:06.417634010 CEST	59444	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:06:06.437268972 CEST	53	59444	8.8.8.8	192.168.2.4
Sep 28, 2022 12:06:13.048048019 CEST	55570	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:06:13.068151951 CEST	53	55570	8.8.8.8	192.168.2.4
Sep 28, 2022 12:06:19.236522913 CEST	64906	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:06:19.258580923 CEST	53	64906	8.8.8.8	192.168.2.4
Sep 28, 2022 12:06:26.661247015 CEST	59446	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:06:26.681572914 CEST	53	59446	8.8.8.8	192.168.2.4
Sep 28, 2022 12:06:32.576051950 CEST	50861	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:06:32.596954107 CEST	53	50861	8.8.8.8	192.168.2.4
Sep 28, 2022 12:06:40.038276911 CEST	61088	53	192.168.2.4	8.8.8.8
Sep 28, 2022 12:06:40.061974049 CEST	53	61088	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 28, 2022 12:05:00.383311987 CEST	192.168.2.4	8.8.8.8	0xe537	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:11.635108948 CEST	192.168.2.4	8.8.8.8	0x7818	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:21.996689081 CEST	192.168.2.4	8.8.8.8	0x659e	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:32.530100107 CEST	192.168.2.4	8.8.8.8	0xa26c	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:39.939918041 CEST	192.168.2.4	8.8.8.8	0x27ff	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:47.937693119 CEST	192.168.2.4	8.8.8.8	0x9118	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:53.971554041 CEST	192.168.2.4	8.8.8.8	0x1d50	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:00.200548887 CEST	192.168.2.4	8.8.8.8	0x821e	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:06.417634010 CEST	192.168.2.4	8.8.8.8	0xd8e2	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:13.048048019 CEST	192.168.2.4	8.8.8.8	0x2205	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:19.236522913 CEST	192.168.2.4	8.8.8.8	0x609e	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:26.661247015 CEST	192.168.2.4	8.8.8.8	0x6b99	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false

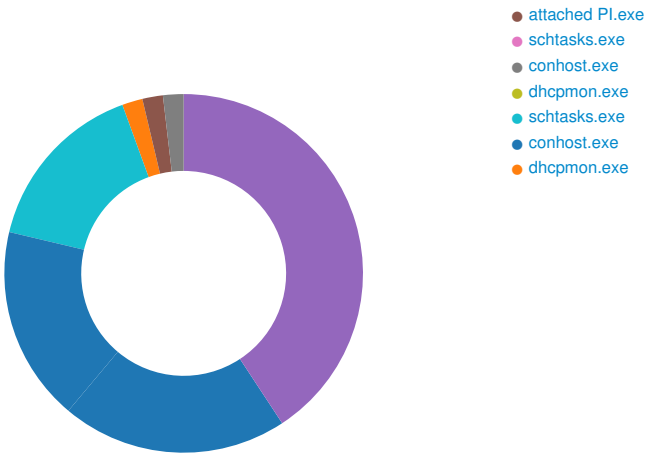
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 28, 2022 12:06:32.576051950 CEST	192.168.2.4	8.8.8.8	0x5187	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:40.038276911 CEST	192.168.2.4	8.8.8.8	0x707b	Standard query (0)	brightnano 1.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 28, 2022 12:05:00.403003931 CEST	8.8.8.8	192.168.2.4	0xe537	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:11.654015064 CEST	8.8.8.8	192.168.2.4	0x7818	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:22.016352892 CEST	8.8.8.8	192.168.2.4	0x659e	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:32.551434040 CEST	8.8.8.8	192.168.2.4	0xa26c	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:39.963004112 CEST	8.8.8.8	192.168.2.4	0x27ff	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:47.957211018 CEST	8.8.8.8	192.168.2.4	0x9118	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:05:53.992727041 CEST	8.8.8.8	192.168.2.4	0x1d50	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:00.220154047 CEST	8.8.8.8	192.168.2.4	0x821e	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:06.437268972 CEST	8.8.8.8	192.168.2.4	0xd8e2	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:13.068151951 CEST	8.8.8.8	192.168.2.4	0x2205	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:19.258580923 CEST	8.8.8.8	192.168.2.4	0x609e	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:26.681572914 CEST	8.8.8.8	192.168.2.4	0x6b99	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:32.596954107 CEST	8.8.8.8	192.168.2.4	0x5187	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false
Sep 28, 2022 12:06:40.061974049 CEST	8.8.8.8	192.168.2.4	0x707b	No error (0)	brightnano 1.ddns.net		171.22.30.170	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: attached PI.exe PID: 1604, Parent PID: 6092

General

Target ID:	3
Start time:	12:04:33
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\attached PI.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\attached PI.exe"
Imagebase:	0xb50000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.330758176.0000000003F59000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.330758176.0000000003F59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.330758176.0000000003F59000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.330758176.0000000003F59000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.331952602.000000000409E000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.331952602.000000000409E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.331952602.000000000409E000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.331952602.000000000409E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000003.00000002.328075400.0000000002F51000.00000004.00000800.00020000.00000000.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	6D83CF06	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	6D83CF06	unknown
C:\Users\user\AppData\Roaming\ecCUXmnB.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C681E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE760.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C687038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\attached PI.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB4C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE760.tmp	success or wait	1	6C686A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ecCUXmnB.exe	0	1131520	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 10 00 00 fd 00 00 00 00 00 00 fd fd 10 00 00 20 00 00 00 fd 10 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 11 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELP @ @	success or wait	1	6C681B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE760.tmp	0	1641	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\attached PI.exe.log	0	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB4C907	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	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Users\user\Desktop\attached PI.exe	unknown	1131520	success or wait	1	6C681B4F	ReadFile

Analysis Process: schtasks.exe PID: **3836**, Parent PID: **1604**

General

Target ID:	7
Start time:	12:04:48
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmpE760.tmp
Imagebase:	0xce0000
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\tmpE760.tmp	unknown	2	success or wait	1	CEAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE760.tmp	unknown	1642	success or wait	1	CEABD9	ReadFile

Analysis Process: conhost.exe PID: **6068**, Parent PID: **3836**

General

Target ID:	8
Start time:	12:04:49
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: attached PI.exe PID: **3092**, Parent PID: **1604**

General

Target ID:	9
Start time:	12:04:50
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\attached PI.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3d0000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: attached PI.exe PID: **4748**, Parent PID: **1604**

General

Target ID:	10
Start time:	12:04:51
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\attached PI.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa40000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.587910914.00000000070F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.574582318.0000000003E61000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588566873.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588566873.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588566873.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588566873.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.575917734.0000000003FE2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.575917734.0000000003FE2000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.575917734.0000000003FE2000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.589359423.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.589359423.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.589359423.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.589359423.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588307356.0000000007270000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588307356.0000000007270000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588307356.0000000007270000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588307356.0000000007270000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.324119603.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.324119603.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.324119603.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000000.324119603.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.587511631.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.587511631.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.587511631.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.587511631.00000000070C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588382533.0000000007280000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588382533.0000000007280000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588382533.0000000007280000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588382533.0000000007280000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588486274.0000000007290000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588486274.0000000007290000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588486274.0000000007290000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588486274.0000000007290000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.578123416.000000000414E000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.578123416.000000000414E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.583841977.00000000059A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.583841977.00000000059A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.583841977.00000000059A0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.583841977.00000000059A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.583841977.00000000059A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588135016.0000000007250000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588135016.0000000007250000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588135016.0000000007250000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588135016.0000000007250000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.563358454.0000000002EA9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.563358454.0000000002EA9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000003.347369078.00000000066EA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.583276687.0000000005530000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.583276687.0000000005530000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.583276687.0000000005530000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.583276687.0000000005530000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588238329.0000000007260000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588238329.0000000007260000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588238329.0000000007260000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588238329.0000000007260000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588938112.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588938112.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588938112.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588938112.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.586982488.0000000006920000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.586982488.0000000006920000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.586982488.0000000006920000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.586982488.0000000006920000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.588818445.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.588818445.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.588818445.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.588818445.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.577106409.00000000040AA000.00000004.00000800.00020000.00000000.sdmp,

	Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.577106409.00000000040AA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D83CF06	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	6D83CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C68BEFF	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	6C681E60	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	6C68BEFF	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	6C68DD66	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	6C68DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD63A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C687038	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	6C681E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpD9B5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C687038	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	6C68BEFF	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	6C68BEFF	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	8	6C681E60	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	6C681E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6C681E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD63A.tmp	success or wait	1	6C686A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD9B5.tmp	success or wait	1	6C686A95	DeleteFileW
C:\Users\user\Desktop\attached PI.exe:Zone.Identifier	success or wait	1	6C602935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 53 fd fd 38 fd fd 48	S8H	success or wait	1	6C681B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 10 00 00 fd 00 00 00 00 00 00 fd fd 10 00 00 20 00 00 00 fd 10 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 fd 11 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELP @ @	success or wait	5	6C68DD66	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	6C68DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD63A.tmp	0	1301	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	38	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 61 74 74 61 63 68 65 64 20 50 49 2e 65 78 65	C:\Users\user\Desktop\attached PI.exe	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpD9B5.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6C681B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	13	6C681B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6C681B4F	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	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D7FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D7FD72F	unknown
C:\Users\user\Desktop\attached PI.exe	unknown	4096	success or wait	1	6D7FD72F	unknown
C:\Users\user\Desktop\attached PI.exe	unknown	512	success or wait	1	6D7FD72F	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	6C68646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **4648**, Parent PID: **4748**

General

Target ID:	11
Start time:	12:04:55
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpD63A.tmp
Imagebase:	0xce0000
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\tmpD63A.tmp	unknown	2	success or wait	1	CEAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD63A.tmp	unknown	1302	success or wait	1	CEABD9	ReadFile

Analysis Process: conhost.exe PID: **2904**, Parent PID: **4648**

General

Target ID:	12
Start time:	12:04:55
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **5328**, Parent PID: **4748**

General

Target ID:	13
Start time:	12:04:55
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpD9B5.tmp
Imagebase:	0xce0000
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\tmpD9B5.tmp	unknown	2	success or wait	1	CEAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD9B5.tmp	unknown	1311	success or wait	1	CEABD9	ReadFile

Analysis Process: conhost.exe PID: **5360**, Parent PID: **5328**

General

Target ID:	14
Start time:	12:04:56
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: attached PI.exe PID: **5344**, Parent PID: **1088**

General

Target ID:	15
Start time:	12:04:56
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\attached PI.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\attached PI.exe" 0
Imagebase:	0xa70000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6D83CF06	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	6D83CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp6181.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C687038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6181.tmp	success or wait	1	6C686A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6181.tmp	0	1641	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C681B4F	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	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **4596**, Parent PID: **1088**

General

Target ID:	16
Start time:	12:04:58
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x8b0000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
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	6D83CF06	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	6D83CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp6CEB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C687038	GetTempFileNameW
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	6DB4C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6CEB.tmp	success or wait	1	6C686A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6CEB.tmp	0	1641	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB4C907	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	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **4812**, Parent PID: **3528**

General

Target ID:	17
Start time:	12:05:03
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xc0000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: schtasks.exe PID: **5072**, Parent PID: **5344**

General

Target ID:	18
Start time:	12:05:19
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmp6181.tmp
Imagebase:	0xce0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **1236**, Parent PID: **5072**

General

Target ID:	19
Start time:	12:05:20
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61e220000
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: attached PI.exe PID: **5216**, Parent PID: **5344**

General	
Target ID:	20
Start time:	12:05:21
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\attached PI.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x340000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: attached PI.exe PID: **2192**, Parent PID: **5344**

General	
Target ID:	21
Start time:	12:05:22
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\attached PI.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe70000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.442688511.0000000003421000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.442688511.0000000003421000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000002.442688511.0000000003421000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.445813095.0000000004429000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.445813095.0000000004429000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000002.445813095.0000000004429000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **6132**, Parent PID: **4596**

General	
Target ID:	22
Start time:	12:05:22
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmp6CEB.tmp
Imagebase:	0xce0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5356**, Parent PID: **6132**

General	
Target ID:	23
Start time:	12:05:22
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **4460**, Parent PID: **4596**

General	
Target ID:	24
Start time:	12:05:25
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcb0000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.449651846.00000000034A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.449651846.00000000034A1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000018.00000002.449651846.00000000034A1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **5920**, Parent PID: **4812**

General	
Target ID:	25
Start time:	12:05:30
Start date:	28/09/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ecCUXmnB" /XML "C:\Users\user\AppData\Local\Temp\tmp8C89.tmp
Imagebase:	0xce0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5184**, Parent PID: **5920**

General	
Target ID:	26
Start time:	12:05:31
Start date:	28/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **2620**, Parent PID: **4812**

General	
Target ID:	27
Start time:	12:05:33
Start date:	28/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbf0000
File size:	1131520 bytes
MD5 hash:	238B41E834F3B663584D4788493BC75F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly