ID: 411952
Sample Name:
NAO09009009.exe
Cookbook: default.jbs
Time: 09:43:46
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

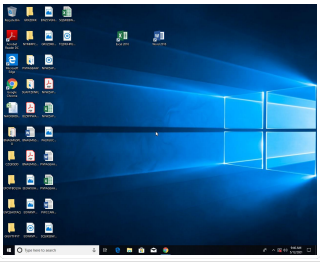
Analysis Report NAO09009009.exe

Overview

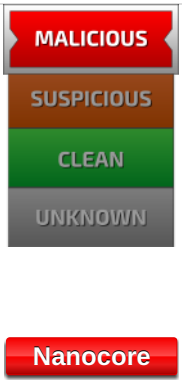
General Information

Sample Name:	NAO09009009.exe
Analysis ID:	411952
MD5:	592b395d837e34..
SHA1:	26498da5dfa5860.
SHA256:	e362816d729cd1..
Tags:	NanoCore
Infos:	

Most interesting Screenshot:



Detection



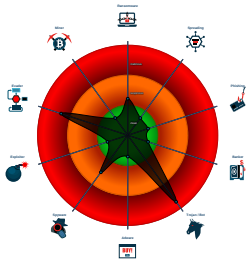
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Uses schtasks.exe or at.exe to add …
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- NAO09009009.exe (PID: 5896 cmdline: 'C:\Users\user\Desktop\NAO09009009.exe' MD5: 592B395D837E34B3770D6113B213B877)
  - MSBuild.exe (PID: 1240 cmdline: 'C:\Users\user\Desktop\NAO09009009.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 5404 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD89D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - conhost.exe (PID: 772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 1264 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpDC18.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 5888 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 4900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6076 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 5312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5404 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2021

```
{
  "Version": "1.2.2.0",
  "Mutex": "2dd052c5-2546-4017-851f-7f690b3c",
  "Group": "Default",
  "Domain1": "185.222.57.171",
  "Domain2": "",
  "Port": 4445,
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.484138546.000000000549 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000002.00000002.484138546.000000000549 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000002.00000002.484247616.000000000572 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000002.00000002.484247616.000000000572 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000002.00000002.484247616.000000000572 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 15 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.MSBuild.exe.3bf9c5e.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d5a7:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d5d4:$x2: IClientNetworkHost

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
2.2.MSBuild.exe.3bf9c5e.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d5a7:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e682:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d5c1:$s5: IClientLoggingHost
2.2.MSBuild.exe.3bf9c5e.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
2.2.MSBuild.exe.3bf9c5e.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xddf:$a: NanoCore • 0xe38:$a: NanoCore • 0xe75:$a: NanoCore • 0xeee:$a: NanoCore • 0x14599:$a: NanoCore • 0x145ae:$a: NanoCore • 0x145e3:$a: NanoCore • 0x2d55d:$a: NanoCore • 0x2d572:$a: NanoCore • 0x2d5a7:$a: NanoCore • 0xe41:$b: ClientPlugin • 0xe7e:$b: ClientPlugin • 0x177c:$b: ClientPlugin • 0x1789:$b: ClientPlugin • 0x14355:$b: ClientPlugin • 0x14370:$b: ClientPlugin • 0x143a0:$b: ClientPlugin • 0x145b7:$b: ClientPlugin • 0x145ec:$b: ClientPlugin • 0x2d319:$b: ClientPlugin • 0x2d334:$b: ClientPlugin
2.2.MSBuild.exe.3bfea94.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 33 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

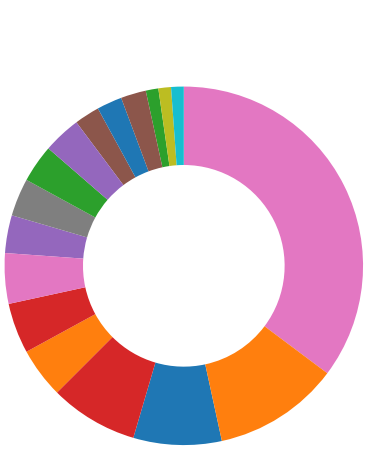
Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for sample

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

- Maps a DLL or memory area into another process
- Writes to foreign memory regions

Copyright Joe Security LLC 2021

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

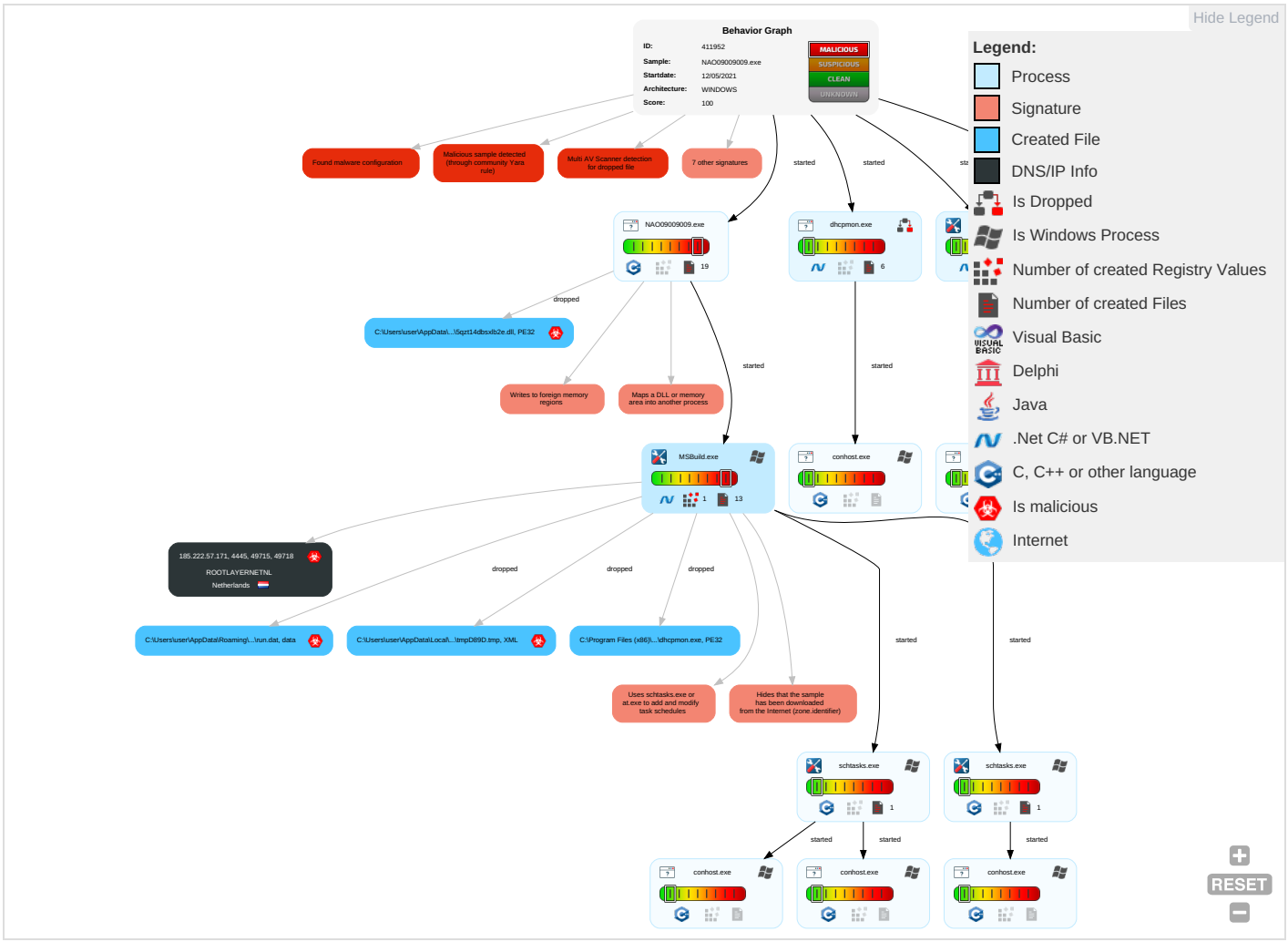
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

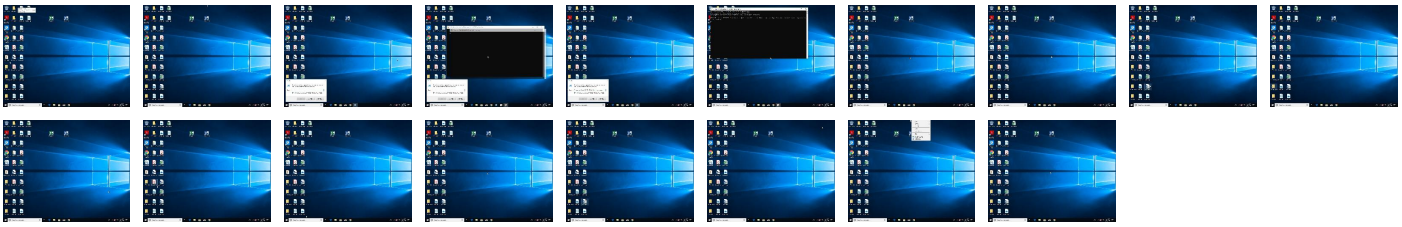
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NAO09009009.exe	33%	Virustotal		Browse
NAO09009009.exe	34%	ReversingLabs	Win32.Backdoor.NanoBot	
NAO09009009.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsoCA66.tmp\5qzt14dbsxlb2e.dll	26%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.MSBuild.exe.5720000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2021

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
185.222.57.171	5%	Virustotal		Browse
185.222.57.171	0%	Avira URL Cloud	safe	
http://go.microsoft.	0%	URL Reputation	safe	
http://go.microsoft.	0%	URL Reputation	safe	
http://go.microsoft.	0%	URL Reputation	safe	
http://go.microsoft.	0%	URL Reputation	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

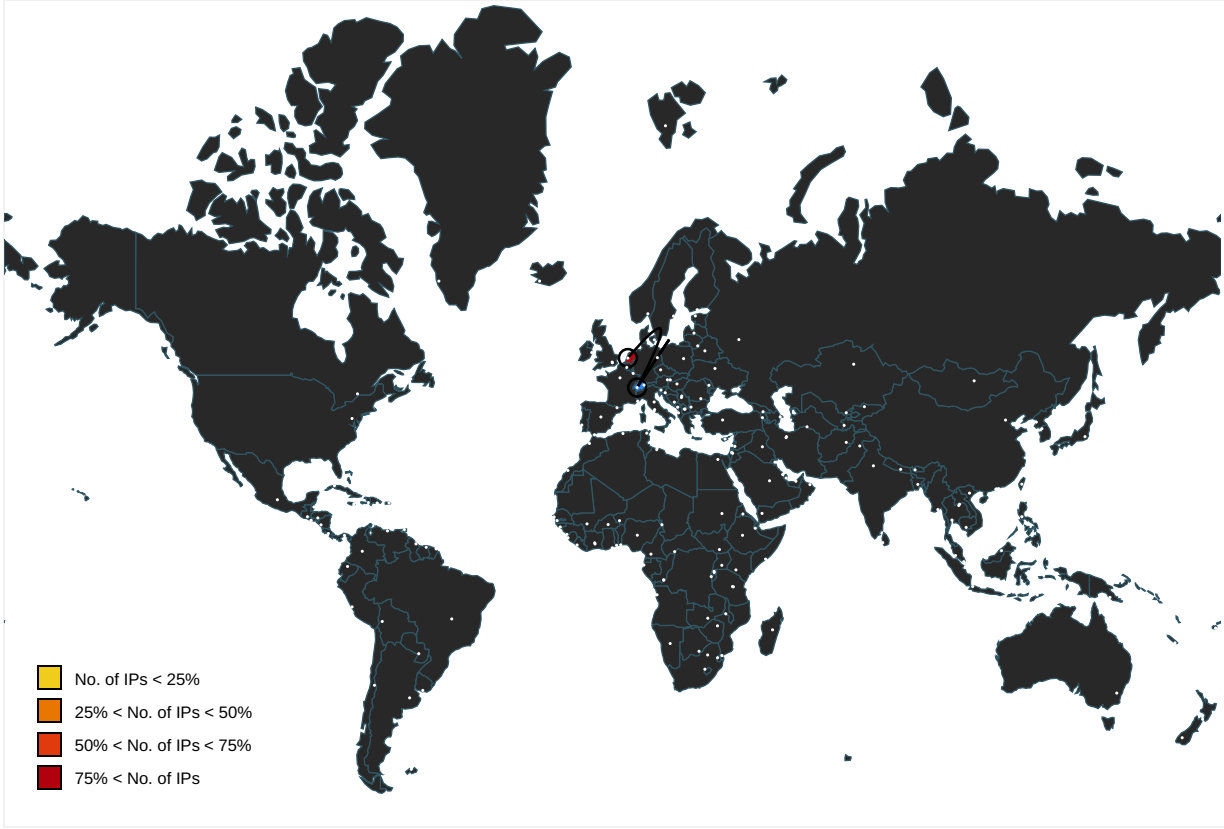
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
185.222.57.171	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://go.microsoft.	dhcpmon.exe, 00000009.00000002.226502855.000000000129C000.00000004.00000020.sdmp, dhcpmon.exe, 0000000B.00000002.239160267.0000000001132000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	NAO09009009.exe	false		high
http://go.microsoft.LinkId=42127	dhcpmon.exe, 00000009.00000002.226502855.000000000129C000.00000004.00000020.sdmp, dhcpmon.exe, 0000000B.00000002.239160267.0000000001132000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.57.171	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411952
Start date:	12.05.2021
Start time:	09:43:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NAO09009009.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/14@0/1
EGA Information:	Failed

Copyright Joe Security LLC 2021

HDC Information:	• Successful, ratio: 46.4% (good quality ratio 45.1%) • Quality average: 86.2% • Quality standard deviation: 23.2%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.147.198.201, 104.43.193.48, 20.82.209.183, 184.30.20.56, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.142.210, 2.20.143.131, 2.20.143.23, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:44:42	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:44:43	API Interceptor	978x Sleep call for process: MSBuild.exe modified
09:44:44	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)
09:44:44	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.222.57.171	SYT09009.exe	Get hash	malicious	Browse	
	EyOVPbKPk5.exe	Get hash	malicious	Browse	
	AS90800009000000.exe	Get hash	malicious	Browse	
	090090000000.exe	Get hash	malicious	Browse	
	fatura 893454.pdf.exe	Get hash	malicious	Browse	
	0997430988.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	SYT09009.exe	Get hash	malicious	Browse	• 185.222.57.171
	shipment documents.jar	Get hash	malicious	Browse	• 185.222.58.147
	EyOVPbKPk5.exe	Get hash	malicious	Browse	• 185.222.57.171
	F14 PO pdf.jar	Get hash	malicious	Browse	• 185.222.58.147
	AS90800009000000.exe	Get hash	malicious	Browse	• 185.222.57.171
	FATOUOO000.exe	Get hash	malicious	Browse	• 185.222.58.152
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 45.137.22.107
	90800000900.exe	Get hash	malicious	Browse	• 45.137.22.107
	fixxing.exe	Get hash	malicious	Browse	• 45.137.22.50
	note-mxm.exe	Get hash	malicious	Browse	• 45.137.22.50
	purchase order confirmation.exe	Get hash	malicious	Browse	• 45.137.22.50
	purchase order acknowledgement.exe	Get hash	malicious	Browse	• 45.137.22.50
	TBBurmah Trading Co., Ltd - products inquiry .exe	Get hash	malicious	Browse	• 45.137.22.50
	FRIEGHT PAYMENT 41,634.20 USD..exe	Get hash	malicious	Browse	• 45.137.22.107
	Due Invoices.exe	Get hash	malicious	Browse	• 45.137.22.107
	PURCHASE ORDER - #0022223 DATED 29042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	PURCHASE ORDER - #0022223, date29042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	B_N SAO SWIFT MT103.exe	Get hash	malicious	Browse	• 45.137.22.50
	PO0900009.exe	Get hash	malicious	Browse	• 185.222.58.152
	PURCHASE ORDER - #0022223 DATED 28042021.exe	Get hash	malicious	Browse	• 45.137.22.50

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	SYT09009.exe	Get hash	malicious	Browse	
	RFQEMFA.Elektrik.exe	Get hash	malicious	Browse	
	cotizaci#U00f3n.PDF.exe	Get hash	malicious	Browse	
	MT103 Slip.exe	Get hash	malicious	Browse	
	Bank details.exe	Get hash	malicious	Browse	
	Shandong CIRS Form.exe	Get hash	malicious	Browse	
	Placement approval.exe	Get hash	malicious	Browse	
	filespdf.exe	Get hash	malicious	Browse	
	goood.exe	Get hash	malicious	Browse	
	Orden n.#U00ba STL21119, pdf.exe	Get hash	malicious	Browse	
	Orden n.#U00ba 21115, pdf.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	DFR2154747.vbe	Get hash	malicious	Browse	
	SOA Dec2020.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Mikey.117100.12986.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe	Get hash	malicious	Browse	
	Purchase Order PDF pdf.exe	Get hash	malicious	Browse	
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	69632

Copyright Joe Security LLC 2021

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Entropy (8bit):	5.20894581699571
Encrypted:	false
SSDEEP:	768:NElGiBcBuiyFjUwF0wdP9/rJMDnRFRJfStGpwV3e3qtAcy:ilGBu7jjP9/tMDn9Jt+VO3GO
MD5:	88BBB7610152B48C2B3879473B17857E
SHA1:	0F6CF8DD66AA58CE31DA4E8AC0631600EF055636
SHA-256:	2C7ACC16D19D076D67E9F1F37984935899B79536C9AC6EEC8850C44D20F87616
SHA-512:	5BACDF6C190A76C2C6A9A3519936E08E898AC8A2B1384D60429DF850BE778860435BF9E5EB316517D2345A5AAE201F369863F7A242134253978BCB5B2179CA58
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SYT09009.exe, Detection: malicious, Browse • Filename: RFQEMFA.Elektrik.exe, Detection: malicious, Browse • Filename: cotizaci#U00f3n.PDF.exe, Detection: malicious, Browse • Filename: MT103 Slip.exe, Detection: malicious, Browse • Filename: Bank details.exe, Detection: malicious, Browse • Filename: Shandong CIRS Form.exe, Detection: malicious, Browse • Filename: Placement approval.exe, Detection: malicious, Browse • Filename: filespdf.exe, Detection: malicious, Browse • Filename: goood.exe, Detection: malicious, Browse • Filename: Orden n.#U00ba STL21119, pdf.exe, Detection: malicious, Browse • Filename: Orden n.#U00ba 21115, pdf.exe, Detection: malicious, Browse • Filename: PO-WJO-001, pdf.exe, Detection: malicious, Browse • Filename: DFR2154747.vbe, Detection: malicious, Browse • Filename: SOA Dec2020.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Mikey.117100.12986.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe, Detection: malicious, Browse • Filename: Purchase Order PDF pdf.exe, Detection: malicious, Browse • Filename: Orden CW62125Q, pdf.exe, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....@..... .....@.. .....@.....99.. ..@.....S.....`/..... ..... ..... ..H.....text..... ..... ..`.rsrc...`/.....0.....@..@.reloc..... . .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	325
Entropy (8bit):	5.334380084018418
Encrypted:	false
SSDEEP:	6:Q3LadLCR22IAQykdL1tZbLsbFLIP12MUAvvro6ysGMFLIP12MUAvvrs:Q3LaJU20NaL1tZbgbe4MqJsGMe4M6
MD5:	65CE98936A67552310EFE2F0FF5BDF88
SHA1:	8133653A6B9A169C7496ADE315CED322CFC3613A
SHA-256:	682F7C55B1B6E189D17755F74959CD08762F91373203B3B982ACFFCADE2E871A
SHA-512:	2D00AC024267EC384720A400F6D0B4F7EDDF49FAF8AB3C9E6CBFBBAE90ECADACA9022B33E3E8EC92E4F57C7FC830299C8643235EB4AA7D8A6AFE9DD1775F5 7C3
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	441
Entropy (8bit):	5.388715099859351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U2+gYhD5itZbgbe4MqJsGMe4M6:MLF20NaL32+g2OH4xvn4j
MD5:	88F0104DB9A3F9BC4F0FC3805F571B0D
SHA1:	CDD4F34385792F0CCE0A844F4ABB447C25AB4E73
SHA-256:	F6C11D3D078ED73F2640DA510E68DEEAA5F14F79CAE2E23A254B4E37C7D0230F
SHA-512:	04B977F63CAB8DE20EA7EFA9D4299C2E625D92FA6D54CA03EECD9F322E978326B353824F23BEC0E712083BDE0DBC5CC4EE90922137106B096050CA46A166DF E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\nsdCA26.tmp	
Process:	C:\Users\user\Desktop\NAO09009009.exe
File Type:	data
Category:	dropped
Size (bytes):	232699
Entropy (8bit):	7.9458235958445975
Encrypted:	false
SSDEEP:	6144:fYBGR9+zLRHHtBFi+StSPBG/gIT6+ZgfNvUrGXFkE8UFUo5:gB3zhtBSesb6CgfNvxkE1t
MD5:	BFBA87CE8CA843AA02E81A2289ECB113
SHA1:	E1E727DA17C004DC2B4A58C9E712677B68339F93
SHA-256:	9C9EF994D63DEC90825F6F3EC91C81284CD9A51B6F1F8EEB542C11AC05E16D05
SHA-512:	6B52BBC1279D3A8DD01536D7B509025A35CF347D846763DC2F394B43288ABD294D8E9A82E7940FBFB8F5D15AB8776773DC9A79F7F8A0B622890E72049BCF509
Malicious:	false
Preview:	.....,.....d..... ....G.....j..... ....

C:\Users\user\AppData\Local\Temp\nsoCA66.tmp\5qzt14dbsxlb2e.dll	
Process:	C:\Users\user\Desktop\NAO09009009.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.633293990487776
Encrypted:	false
SSDEEP:	48:qV++kltvwuvDujtEzqwUQgMR2u5lNd/Z3Gmh:qkHvjDNmw/8u7Hnh
MD5:	3BFC96F1A112C283B6585A4CE0C7D189
SHA1:	061A77A69DCA69D2A344A908EBF8598921DD5FFA
SHA-256:	1CBF681459CACFDCAFE28399CA2BB190CE556A573436C8A2B205ABAFB62D948E
SHA-512:	1779FE59F5A09408B039B126FCC2E2E273525458D61184FB217E056C97EDC73F541693C01F7C7AA116368294864FD8781642B7611D820456A5113281A58D74D7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.`..... .!..... .....@.....$..K.... ..... .....text..... ..`.rdata..... .....@..@.data... ....0.....@..... .....

C:\Users\user\AppData\Local\Temp\q1do00rflcztdt	
Process:	C:\Users\user\Desktop\NAO09009009.exe
File Type:	data
Category:	dropped
Size (bytes):	15877
Entropy (8bit):	7.987428846489735
Encrypted:	false
SSDEEP:	384:qPV4M3TqyXeFbtRGwo/pSnfM6R4uHlZbmUnFoWHouj89n4:qiM3dcf2pSfZR1HnbmyrHouj89n4
MD5:	24BD111E1EDB9B67A16668B909F37B80
SHA1:	6706B953B5D1B4C211A4DDD0926B380776C3CA1A
SHA-256:	5B454CCD88BC78732CE6B6A40FEC0BBBC5FDEE4191F94ABF0B8DAD8AD06DB629
SHA-512:	08F9CAD39D360AC5EE34E4CFA1FEA6DBBE6E2EA87481D69A3643891507E27B94C815917F0A02F24F71BA55C7667771534B69FB008806D832894E01F602B59F23
Malicious:	false
Preview:	I.p....\.%q...9t.sK.z...t...h.....I....p.}J.~...{I.{..'..N.....;.|.R...C....|._LI.D...?...=..I@.....;.e.U.....a.HAa.A.....2."..p9.....{.z.H...E...V.}Ff.Ft,.-...?.>C>.....r.C.S...J.}.c.BSs.[...*...<.. Z.....R.p.F...W.u.p.SpP0X,..3...1..E4...../.i.I...D...u.LUu.U.....6..Z|-.....&.n.\...Y.f..z.IZz.Zm8.1.5.#.-O".....G.G...^ ,..w.^Gg._...>..@ ..V.....d.J...[...d.wTt.\...'./.%..Q(.... ...}.M...H...i.`li.I..,...*.0h1.....r.P...M.#.^.eNn.N.$.%...7..K6.....[.K...R....{.JKk.C.'.2...$..B/.....x.^...O...x.[Xx.P"..;...9.eM<.....a.a...L...}.t(..hnK....f3.R%.~..z...._.....*.....?..CK~n. [{b..../...4..s....f.....&..^HyC.Hh}.=..*#8.).....i.....=..QMdX.Mmx.:.@)23.....%.W7..K6...g...TQ)....[.....t/q%..IUL....o._.....x|-.....r...QP"..;.:.z-.'..[Sf^.Ccz.0..7...,.. k....~...J.....>..F`aC.`e.5..".@.!.Yx....a.....5..YElX.Ee..2.8!.;.&..I.....f.C.S..J..r7.I..3...'...<?6..Mmx.

C:\Users\user\AppData\Local\Temp\tmpD89D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320

C:\Users\user\AppData\Local\Temp\tmpD89D.tmp	
Entropy (8bit):	5.136963558289723
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnc2xtn:cbk4oL600QydbQxIYODOLedq3ZLj
MD5:	AE766004C0D8792953BAFFFE8F6A2E3B
SHA1:	14B12F27543A401E2FE0AF8052E116CAB0032426
SHA-256:	1ABDD9B6A6B84E4BA1AF1282DC84CE276C59BA253F4C4AF05FEA498A4FD99540
SHA-512:	E530DA4A5D4336FC37838D0E93B5EB3804B9C489C71F6954A47FC81A4C655BB72EC493E109CF96E6E3617D7623AC80697AD3BBD5FFC6281BAFC8B34DCA5E657
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpDC18.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\yw4e566wncbxyt	
Process:	C:\Users\user\Desktop\NAO09009009.exe
File Type:	data
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	**7.999202585371924**
Encrypted:	**true**
SSDEEP:	6144:2+zLRHHtBFi+StSPBG/gIT6+ZgfNvUrGXFkE8UFUoW:PzhtBSesb6CgfNvxkE1tW
MD5:	858FF867A327D25FA18931791F3B062E
SHA1:	D072503D61F302AAAC6B711E192AF5F02535F568
SHA-256:	32B1B06E77375392D1204FFB933AB8337D10FC11C22C2069633011998372C5A5
SHA-512:	29F162D83DBB46E1BD25BC99C8088DB29C057BAC5435DF80C000957B41B450AC6E3128C3CB57275198465605527D959B51457BC4F29CD4CBB0D9EBECAAFB328
Malicious:	false
Preview:	C.. .SypS.....q.$S./.M...]O..h..|.r..I.S..|...'Y...X..0..... .._i..]....IO.V:q..fz.O.?.jf}...Oa=..+."..e...].C..<....D0.Y..{7....*..{C.Z.&.x.05s...~&.....M.(...r`....../^w..d&UV..Zb.M...{*...I..8z.4..#R..R....*..../.{...v.~MF!./...6..K0..K..w..F..R[z.j"?ev8.rZ.5.g&..W6..`.....Dh3...9..5rh.\.mD.f.....h.......6.c3:.P..C.....`+.=.A.....}.b.{}..B...d.ny. jX.../..\....=I.. ..9..6..w.p.O.j..e vO.R.Gb.S2..W6$.....QUi ;..jwG."..*.$.........Q.>.T....T.%]&...]......+`.M.]6T...g....j..L...O;..I..+~..A.M.*1.N...;<.....7.......F9[.9.....ok...W......../.?.n.....h.@..>..;.O..?.9.@..p[.....*g..S":.....{...fL.....#..Z..`....2L5.:.....o..U0.*.(E,.#..]....Y..z...9C`..'...M.....x.....7"....NU.;.)...+w...8.........3..5.5..5(G..v.=.....e...P....gf.....W....=Z..t.7y.k[...-2gu..w....j..!|..A?4...n..... ..XP.c6V|.....:2p.o..<.....Rm.<...0.}q..-}cNh.M.....@.._.s;..e.3M#.F....L:_.+(....V!.hSt.....t..X<<.....T._/.....4k.Sd.BS"..B(..u..2.S.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Eq:R
MD5:	B7F8B97632E6216C1F0F73EA5DD90CC1

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA1:	BDE7507A816875E5FD1BF7FE63870814AE874231
SHA-256:	D7BD87BDD316B1C3E51C0A384C58836AFB9553F95343E3A47974229F55C02DD2
SHA-512:	3ADB9F12EEEC3918FB2D0F12791ECFEFF8BE85628C81B2728EB2348A01AD6FF44B897E29C8CDBADB28FF0E53E49253491570560E03557CF2AECB0FA37C7D4ED7
Malicious:	**true**
Preview:	2i.=e..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.85263908467479
Encrypted:	false
SSDEEP:	3:oMty8WbSI1u:oMLWuI1u
MD5:	A35128E4E28B27328F70E4E8FF482443
SHA1:	B89066B2F8DB34299AABFD7ABEE402D5444DD079
SHA-256:	88AEA00733DC4B570A29D56A423CC5BF163E5ACE7AF349972EB0BBA8D9AD06E1
SHA-512:	F098E844B5373B34642B49B6E0F2E15CFDAA1A8B6CABC2196CEC0F3765289E5B1FD4AB588DD65F97C8E51FA9A81077621E9A06946859F296904C646906A70F33
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.969261552825097
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFdCsq2UTiMdH8stCal+n:zK1XnV30ZsGMIG9BFRbQdCT2UftCM+
MD5:	F227448515085A647910907084E6728E
SHA1:	5FA1A8E28B084DA25A1BBC51A2D75810CEF57E2C
SHA-256:	662BA47D628FE8EBE95DD47B4482110A10B49AED09387BC0E028BB66E68E20BD
SHA-512:	6F6E5DFFF7B17C304FB19B0BA5466AF84EF98A5C2EFA573AF72CFD3ED6964E9FD7F8E4B79FCFFBEF87CE545418C69D4984F4DD60BBF457D0A3640950F8FC5AF0
Malicious:	false
Preview:	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.827750389453101
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	NAO09009009.exe
File size:	283759
MD5:	592b395d837e34b3770d6113b213b877
SHA1:	26498da5dfa58609b38a6f0d294d35e60608cb78
SHA256:	e362816d729cd17eeca2ca5361937558f0455463bf4fba74d220163c43f46308
SHA512:	8545fa49f2c7a11bc619e79bf782ae85183a0430b1a79d742a2a66f9e4d39768aca5eab66d56d1c3414200edc4e5806d01a5bfc3e23a2e351986a5add9afc7f0
SSDEEP:	6144:jgORakB1sWrqD1jMeImmPaEBcrdNvBVcI15AArbVKWJua:jgI1sWrqRnIhiEOdVLnA+JH

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....$_.....f...*.....

File Icon

Icon Hash:	e4e6b292a4b4bcb4

Static PE Info

General

Entrypoint:	0x4035d8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D702 [Sat Aug 1 02:44:18 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c05041e01f84e1ccca9c4451f3b6a383

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080C8h]
call dword ptr [004080CCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042A26Ch], eax
je 00007F4D4493F713h
push ebx
call 00007F4D44942A19h
cmp eax, ebx
je 00007F4D4493F709h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F4D44942993h
push esi
call dword ptr [00408154h]
lea esi, dword ptr [esi+eax+01h]

Instruction
cmp byte ptr [esi], 00000000h
jne 00007F4D4493F6ECh
push 0000000Bh
call 00007F4D449429ECh
push 00000009h
call 00007F4D449429E5h
push 00000007h
mov dword ptr [0042A264h], eax
call 00007F4D449429D9h
cmp eax, ebx
je 00007F4D4493F711h
push 0000001Eh
call eax
test eax, eax
je 00007F4D4493F709h
or byte ptr [0042A26Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408298h]
mov dword ptr [0042A338h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 00421708h
call dword ptr [0040818Ch]
push 0040A384h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x6010	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6572	0x6600	False	0.662300857843	data	6.45391938596	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1398	0x1400	False	0.449609375	data	5.13671758274	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.5078125	data	4.09680908363	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b000	0x6010	0x6200	False	0.451769770408	data	5.54913124873	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b280	0x25a8	data	English	United States
RT_ICON	0x3d828	0x10a8	data	English	United States
RT_ICON	0x3e8d0	0xea8	data	English	United States
RT_ICON	0x3f778	0x8a8	data	English	United States
RT_ICON	0x40020	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x40588	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x409f0	0x100	data	English	United States
RT_DIALOG	0x40af0	0x11c	data	English	United States
RT_DIALOG	0x40c10	0x60	data	English	United States
RT_GROUP_ICON	0x40c70	0x5a	data	English	United States
RT_MANIFEST	0x40cd0	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

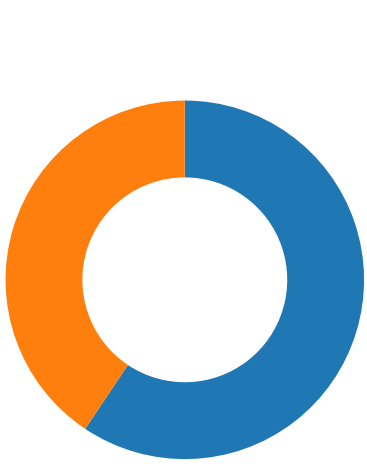
DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetWindowLongW, GetSysColor, SetWindowPos, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersion, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, ExitProcess, CopyFileW, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 09:44:29.477237940 CEST	49698	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.491261959 CEST	49699	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.512136936 CEST	49701	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.534522057 CEST	443	49698	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.534720898 CEST	443	49698	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.534754038 CEST	443	49698	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.534852028 CEST	49698	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.534882069 CEST	49698	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.536649942 CEST	443	49698	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.536694050 CEST	443	49698	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.536758900 CEST	49698	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.536789894 CEST	49698	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.538896084 CEST	443	49698	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.538988113 CEST	49698	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.545105934 CEST	49700	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.547403097 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.547899008 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.547925949 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.547950029 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.547965050 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.547986031 CEST	49699	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.548022032 CEST	49699	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.567554951 CEST	443	49701	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.568203926 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.568361044 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.570080042 CEST	443	49701	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.570108891 CEST	443	49701	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.570125103 CEST	443	49701	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.570157051 CEST	443	49701	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.570173025 CEST	443	49701	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.570183039 CEST	49701	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.570266008 CEST	49701	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.590218067 CEST	49699	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.600667953 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.600966930 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.600995064 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.601016045 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.601038933 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.601058960 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.601058960 CEST	49700	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.601082087 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.601098061 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.601124048 CEST	49700	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.601171017 CEST	49700	443	192.168.2.3	92.122.145.220

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 09:44:29.613279104 CEST	49700	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.615782976 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615816116 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615827084 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615837097 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615852118 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615869045 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615885973 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615902901 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615919113 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.615932941 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.616024017 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.616106987 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.645822048 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.646908998 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.646943092 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.647018909 CEST	49699	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.647061110 CEST	49699	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.648627996 CEST	443	49699	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.648711920 CEST	49699	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.663728952 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.663768053 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.663794994 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.663820028 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.663855076 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.663887024 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.663935900 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.663965940 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.664012909 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.664040089 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.664067984 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.664093971 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.664127111 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.664164066 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.664176941 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.664187908 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.664223909 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.664247990 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.664284945 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.664309025 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.664351940 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.669001102 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.670507908 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.670558929 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.681108952 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.681159973 CEST	443	49700	92.122.145.220	192.168.2.3
May 12, 2021 09:44:29.681308031 CEST	49700	443	192.168.2.3	92.122.145.220
May 12, 2021 09:44:29.712960005 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.713013887 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.713059902 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.713099003 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.713135958 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.713172913 CEST	443	49689	131.253.33.200	192.168.2.3
May 12, 2021 09:44:29.713238955 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.713263988 CEST	49689	443	192.168.2.3	131.253.33.200
May 12, 2021 09:44:29.718096018 CEST	443	49689	131.253.33.200	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 09:44:28.892548084 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:28.941346884 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 09:44:30.280045033 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:30.328808069 CEST	53	60152	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2021

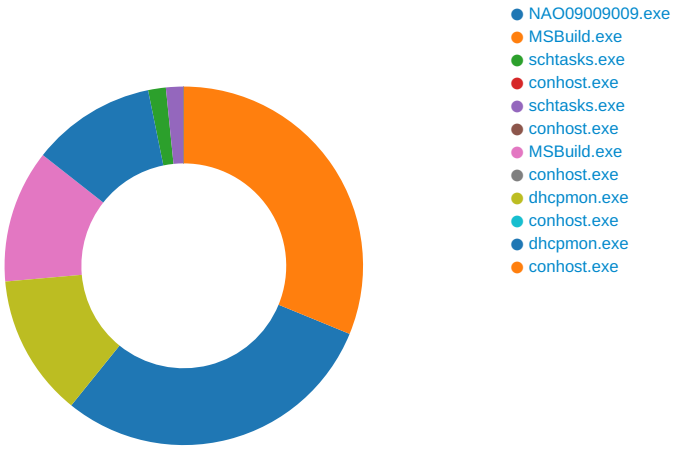
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 09:44:33.119975090 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:33.173728943 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 09:44:34.520463943 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:34.586055994 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 09:44:35.818169117 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:35.868401051 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 09:44:37.162779093 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:37.211580038 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 09:44:38.300517082 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:38.354060888 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 09:44:42.776598930 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:42.834000111 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 09:44:43.757005930 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:43.812577009 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 09:44:44.780057907 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:44.829046965 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 09:44:47.608786106 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:47.660283089 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 09:44:49.955550909 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:50.006314039 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 09:44:51.224637985 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:51.275702000 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 09:44:52.704076052 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:52.753058910 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 09:44:53.841758013 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:53.892168999 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 09:44:56.843431950 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:56.893704891 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 09:44:57.863147020 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:57.912159920 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 09:44:59.025852919 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 09:44:59.077375889 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 09:45:03.918459892 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 09:45:03.993010044 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 09:45:04.259522915 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 09:45:04.350425005 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 09:45:19.328228951 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 09:45:19.390644073 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 09:45:24.734114885 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 09:45:24.793651104 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 09:45:37.273210049 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 09:45:37.332145929 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 09:45:42.478077888 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 09:45:42.536917925 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 09:46:14.662676096 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 09:46:14.730705976 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 09:46:16.464292049 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 09:46:16.521667004 CEST	53	56132	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior

Copyright Joe Security LLC 2021



Click to jump to process

System Behavior

Analysis Process: NAO09009009.exe PID: 5896 Parent PID: 5780

General

Start time:	09:44:37
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\NAO09009009.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NAO09009009.exe'
Imagebase:	0x400000
File size:	283759 bytes
MD5 hash:	592B395D837E34B3770D6113B213B877
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.219500091.0000000000B50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.219500091.0000000000B50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.219500091.0000000000B50000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.219500091.0000000000B50000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsjC9F7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdCA26.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\q1do00rflcztdt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Local\Temp\yw4e566wncbxyt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Local\Temp\nsoCA66.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsoCA66.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405ABC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsoCA66.tmp\5qzt14dbsxlb2e.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsjC9F7.tmp	success or wait	1	403887	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsoCA66.tmp	success or wait	1	405C7D	DeleteFileW

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsdCA26.tmp</td><td>unknown</td><td>24177</td><td>e6 12 00 00 80 00 00
00 2c 01 00 00 02 00
00 00 ac 01 00 00 01
00 00 00 c4 09 00 00
18 00 00 00 64 0c 00
00 00 00 00 00 20 12
00 00 01 00 00 00 e6
12 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00 ff
ff ff ff ff ff ff ff ff ff ff
00 00 00 00 00 ff 00 00
c6 00 00 00 f1 ff ff 00
00 00 00 ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00</td><td>........,.........................d.......
....
....
....
....
....
....
....
................</td><td>success or wait</td><td>14</td><td>4060FE</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\q1do00rflcztdt</td><td>unknown</td><td>15877</td><td>49 e5 b6 70 83 c4 18
ed 5c d1 25 71 da c7
d1 39 74 05 73 4b 05
7a a2 eb 90 0d 74 b1
dd ae ee b4 68 17 98
06 b6 8e 91 88 05 fd
49 b7 e3 9d 13 b7 70
99 7d 4a f6 7e d4 bd 0f
0f 7b 49 b6 7b ad fc 27
81 9a 4e 13 fd 8c df cc
ec 9a f6 3b b5 7c b2
52 86 9b af 43 0d ec
ca c0 7c 17 5f 4c 6c 0c
44 e9 0a db 3f d4 07
1d 3d d0 b6 18 49 40
fa 97 d6 c9 e9 9f db 3b
84 65 b3 55 9b 88 94
80 06 e5 c9 b9 61 02
48 41 61 01 41 00 15
00 04 c7 32 02 22 d5
83 b5 70 39 ef 82 c9
da fa 9c e0 7b 97 7a
a4 48 90 a5 b9 45 1b
fe f0 ba 56 01 7d 46 66
06 46 74 2c f1 2d da
01 1f 3f de a0 3e 43 3e
e4 85 cc d7 f7 99 d5
72 86 43 ad 53 b9 8a
b6 4a 0c 7d e7 ab 63
04 42 53 73 13 5b fe 1f
fe 2a d5 08 1c 3c d3
95 b2 5a 17 e9 90 c3
e0 00 8e f2 52 a1 70
a6 46 8a 8f bb 57 19
75 de ac 70 03 53 70
50 30</td><td>I..p....\.%q...9t.sK.z....t...
..h.........I.....p.}J.~....{I.
{..'..N........;.|.R...C....|
._Ll.D...?...=...I@.......;.e.
U........a.HAa.A.....2."...p9.
......{.z.H...E....V.}Ff.Ft,.-
...?..>C>.......r.C.S...J.}..c
.BSs.[...*...<...Z........R.p.
F...W.u..p.SpP0</td><td>success or wait</td><td>1</td><td>4060FE</td><td>WriteFile</td></tr>
</table>

Copyright Joe Security LLC 2021

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\yw4e566wncbxyt</td><td>unknown</td><td>16384</td><td>43 ed eb 20 ad 53 79
70 53 9b c4 ef 1f 8c e6
71 94 24 53 9e 2f c1
4d bb a0 82 5d 4f dd f7
68 bc b4 7c c5 72 a4
bd 49 0e 53 f2 ed b2
7c df 0e 0f 27 59 e5 d0
d7 91 58 02 97 30 f9
db f4 1b 93 20 dd 1c 5f
69 b9 df 5d fe 06 88 a0
49 4f cb 56 3a 71 d6
de 66 7a fe 4f de 3f d0
6a 66 7d bf d3 8d a3 4f
61 3d be 9f 2b a2 22
b8 11 65 8c 0f 0b 5d
d0 bb 43 96 d0 9f 3c
ec 06 b7 c1 44 30 d6
59 ca d7 7b 37 87 1e
90 d6 2a 06 c4 7b 43
ef 5a cf 26 dc b5 78 8b
30 35 73 e7 b8 bd 1c
c8 7e 26 2e a0 b8 ee
cc 80 4d 01 28 a4 dd
b5 ae 72 60 ad b2 8e
d4 fe fc 5e 77 ee 89 d1
64 26 55 56 1c a2 5a
62 9e 4d 02 e0 93 7b
2a 15 f1 84 d9 a7 6c
d4 1a 38 7a e3 34 89
bb 23 52 d4 b5 96 52
c0 18 cd e1 2a ad d0
f6 01 2f ca 7b b7 04 0f
76 ac 7e 4d 46 21 e3
2f ad 8e c9 36 bf cc a8
4b 30 ab 92 4b f9</td><td>C..
.SypS......q.$S./.M...]O..
h..|.r..I.S...|...'Y....X..0.....
.._i..]....IO.V:q..fz.O.?.
jf}....Oa=..+."..e...]..C...<.
...D0.Y..{7....*..{C.Z.&..x.05
s.....~&......M.(....r`......^
w...d&UV..Zb.M...
{*.....l..8z.4..#R...R....*..../.
{...v.~MF!./...6...K0..K.</td><td>success or wait</td><td>13</td><td>4060FE</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Te
mp\nsoCA66.tmp\5qzt14dbsxlb2e.dll</td><td>unknown</td><td>4096</td><td>4d 5a 90 00 03 00 00
00 04 00 00 00 ff ff 00
00 b8 00 00 00 00 00
00 00 40 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 d0 00 00 00
0e 1f ba 0e 00 b4 09
cd 21 b8 01 4c cd 21
54 68 69 73 20 70 72
6f 67 72 61 6d 20 63
61 6e 6e 6f 74 20 62
65 20 72 75 6e 20 69
6e 20 44 4f 53 20 6d 6f
64 65 2e 0d 0d 0a 24
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 50 45 00 00
4c 01 03 00 ae 44 9b
60 00 00 00 00 00 00
00 00 e0 00 03 21 0b
01 0b 00 00 04 00 00
00 08 00 00 00 00 00
00 00 00 00 00 00 10
00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$............................
....
............................PE
..L....D.`...........!........
..............</td><td>success or wait</td><td>1</td><td>4060FE</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NAO09009009.exe	unknown	512	success or wait	124	4060CF	ReadFile
C:\Users\user\Desktop\NAO09009009.exe	unknown	16384	success or wait	14	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsdCA26.tmp	unknown	4	success or wait	1	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsdCA26.tmp	unknown	4838	success or wait	1	4033F7	ReadFile
C:\Users\user\AppData\Local\Temp\nsdCA26.tmp	unknown	4	success or wait	3	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\q1do00rflcztdt	unknown	15877	success or wait	1	100010CB	ReadFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yw4e566wncbxyt	unknown	207872	success or wait	1	B43092	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B40A62	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B40A62	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B40A62	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B40A62	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B40A62	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B40A62	ReadFile

Analysis Process: MSBuild.exe PID: 1240 Parent PID: 5896

General

Start time:	09:44:38
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NAO09009009.exe'
Imagebase:	0x470000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000002.00000002.484138546.0000000005490000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.484138546.0000000005490000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.484247616.0000000005720000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.484247616.0000000005720000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.484247616.0000000005720000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.475482671.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.475482671.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.475482671.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.482810571.0000000003BF7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.482810571.0000000003BF7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

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	72FB60AC	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	72FB60AC	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	28407A1	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	284089B	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	28407A1	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	2840B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD89D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2840D1C	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	284089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpDC18.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2840D1C	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	28407A1	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	28407A1	CreateDirectoryW
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	72FB60AC	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	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD89D.tmp	success or wait	1	96BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpDC18.tmp	success or wait	1	96BF0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	32 69 97 3d 65 15 d9 48	2i.=e..H	success or wait	1	2840A53	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	69632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 a9 d1 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 c0 00 00 00 40 00 00 00 00 00 00 de d2 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 01 00 00 10 00 00 39 39 01 00 03 00 40 05 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....$.......PE..L..... {Z.....................@........... ....@.. ....@ ......99....@.................	success or wait	1	2840B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD89D.tmp	unknown	1320	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	2840A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	57	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 4d 53 42 75 69 6c 64 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	success or wait	1	2840A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDC18.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	2840A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2840A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	2840A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	2840A53	ReadFile

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	2840C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 5404 Parent PID: 1240

General

Start time:	09:44:42
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD89D.tmp'
Imagebase:	0x1260000
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\tmpD89D.tmp	unknown	2	success or wait	1	126AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD89D.tmp	unknown	1321	success or wait	1	126ABD9	ReadFile

Analysis Process: conhost.exe PID: 968 Parent PID: 5404

General

Start time:	09:44:42
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 1264 Parent PID: 1240

General

Start time:	09:44:42
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpDC18.tmp'
Imagebase:	0x1260000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

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\tmpDC18.tmp	unknown	2	success or wait	1	126AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDC18.tmp	unknown	1311	success or wait	1	126ABD9	ReadFile

Analysis Process: conhost.exe PID: 3732 Parent PID: 1264

General

Start time:	09:44:43
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: MSBuild.exe PID: 5888 Parent PID: 528

General

Start time:	09:44:44
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0
Imagebase:	0x110000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

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	72FB60AC	unknown

Copyright Joe Security LLC 2021

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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	90A7A3	WriteFile
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	90A7A3	WriteFile
\Device\ConDrv	unknown	66	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 39 3a 20 50 72 6f 6a 65 63 74 20 66 69 6c 65 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 0d 0a 53 77 69 74 63 68 3a 20 30 0d 0a	MSBUILD : error MSB1009: Project file does not exist...Switch: 0..	success or wait	1	90A7A3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	unknown	325	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 45 6e 67 69 6e 65 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 46 72 61 6d 65 77 6f 72 6b 2c 20	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework,	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.rsp	unknown	4096	success or wait	1	90A7A3	ReadFile

Analysis Process: conhost.exe PID: 4900 Parent PID: 5888

General

Start time:	09:44:44
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6076 Parent PID: 528

General

Start time:	09:44:44
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xb20000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	10FA897	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922.. [Microsoft .NET Framework, Version 2.0. 50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	10FA897	WriteFile
\Device\ConDrv	unknown	66	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 39 3a 20 50 72 6f 6a 65 63 74 20 66 69 6c 65 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 0d 0a 53 77 69 74 63 68 3a 20 30 0d 0a	MSBUILD : error MSB1009: Project file does not exist...Switch: 0..	success or wait	1	10FA897	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	441	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 58 6d 6c 5c 35 32 37 63 39 33 33 31 39 34 66 33 61 39 39 61 38 31 36 64 38 33 63 36 31 39 61 33 65 31 64 33 5c 53 79 73 74 65 6d 2e 58 6d 6c 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0 .50727_32\System\1ffc437de59fb 69ba2b865ffdc98ffd1\System.ni. dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d8 3c619a3e1d3\System.Xml.ni.dll",0..2,"Microsof	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	10FA897	ReadFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	10FA897	ReadFile

Analysis Process: conhost.exe PID: 5312 Parent PID: 6076

General

Start time:	09:44:45
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 5404 Parent PID: 3388

General

Start time:	09:44:50
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x9e0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	unknown

Copyright Joe Security LLC 2021

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	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	10CA897	WriteFile
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	10CA897	WriteFile
\Device\ConDrv	unknown	137	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 33 3a 20 53 70 65 63 69 66 79 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 20 54 68 65 20 63 75 72 72 65 6e 74 20 77 6f 72 6b 69 6e 67 20 64 69 72 65 63 74 6f 72 79 20 64 6f 65 73 20 6e 6f 74 20 63 6f 6e 74 61 69 6e 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 0d 0a	MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...	success or wait	1	10CA897	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	10CA897	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	10CA897	ReadFile

Analysis Process: conhost.exe PID: 772 Parent PID: 5404

General

Start time:	09:44:51
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC 2021