ID: 411310
Sample Name: SYT09009.exe
Cookbook: default.jbs
Time: 19:39:56
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

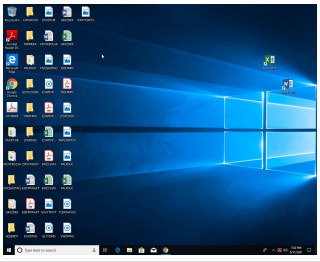
Analysis Report SYT09009.exe

Overview

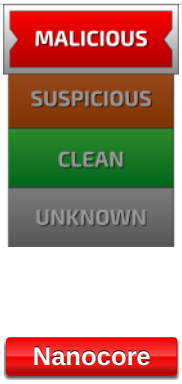
General Information

Sample Name:	SYT09009.exe
Analysis ID:	411310
MD5:	fbfddfc110fd9d37..
SHA1:	250149eebd54c7..
SHA256:	b98a4c0f84e431c..
Tags:	NanoCore
Infos:	

Most interesting Screenshot:



Detection



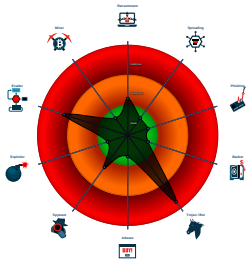
Nanocore

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
- Snort IDS alert for network traffic (e…
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Maps a DLL or memory area into an…
- Uses schtasks.exe or at.exe to add …
- Writes to foreign memory regions
- Checks if Antivirus/Antispyware/Fire…

Classification



Startup

- **System is w10x64**
- SYT09009.exe (PID: 4956 cmdline: 'C:\Users\user\Desktop\SYT09009.exe' MD5: FBFDDFC110FD9D3775674447316DE3D8)
  - MSBuild.exe (PID: 3332 cmdline: 'C:\Users\user\Desktop\SYT09009.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 4320 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA63C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5840 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpA9C7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 5868 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 5872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 4440 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 4684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6140 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 5876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.258062190.000000000404 3000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1d7a:$a: NanoCore • 0x1d9f:$a: NanoCore • 0x1df8:$a: NanoCore • 0x11f95:$a: NanoCore • 0x11fbb:$a: NanoCore • 0x12017:$a: NanoCore • 0x1ee6c:$a: NanoCore • 0x1eec5:$a: NanoCore • 0x1eef8:$a: NanoCore • 0x1f124:$a: NanoCore • 0x1f1a0:$a: NanoCore • 0x1f7b9:$a: NanoCore • 0x1f902:$a: NanoCore • 0x1fdd6:$a: NanoCore • 0x200bd:$a: NanoCore • 0x200d4:$a: NanoCore • 0x2345d:$a: NanoCore • 0x24817:$a: NanoCore • 0x24861:$a: NanoCore • 0x254bb:$a: NanoCore • 0x2aaa0:$a: NanoCore
00000000.00000002.251070693.000000000245 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.251070693.000000000245 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
00000000.00000002.251070693.000000000245 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.251070693.000000000245 0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SYT09009.exe.2450000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.SYT09009.exe.2450000.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.2.SYT09009.exe.2450000.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.SYT09009.exe.2450000.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
1.3.MSBuild.exe.404c416.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
Click to see the 16 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

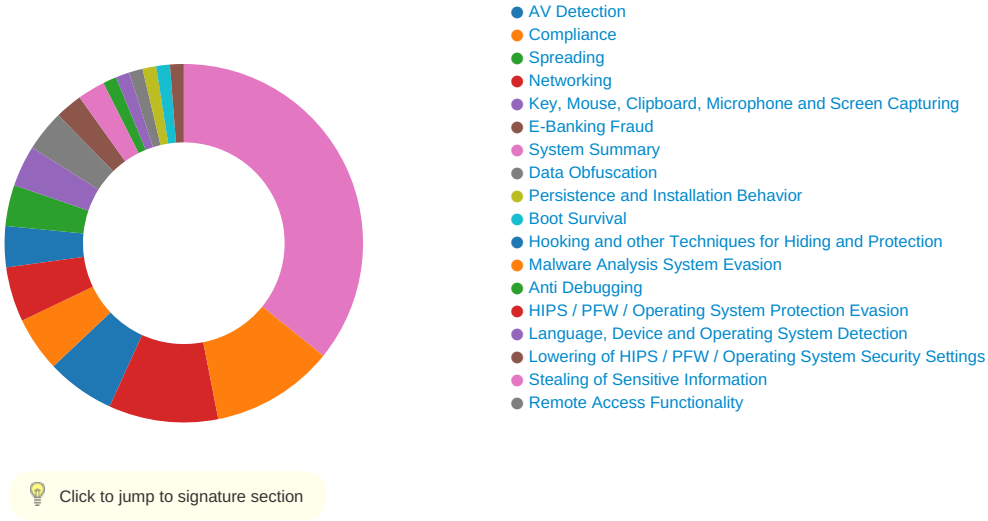
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview



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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

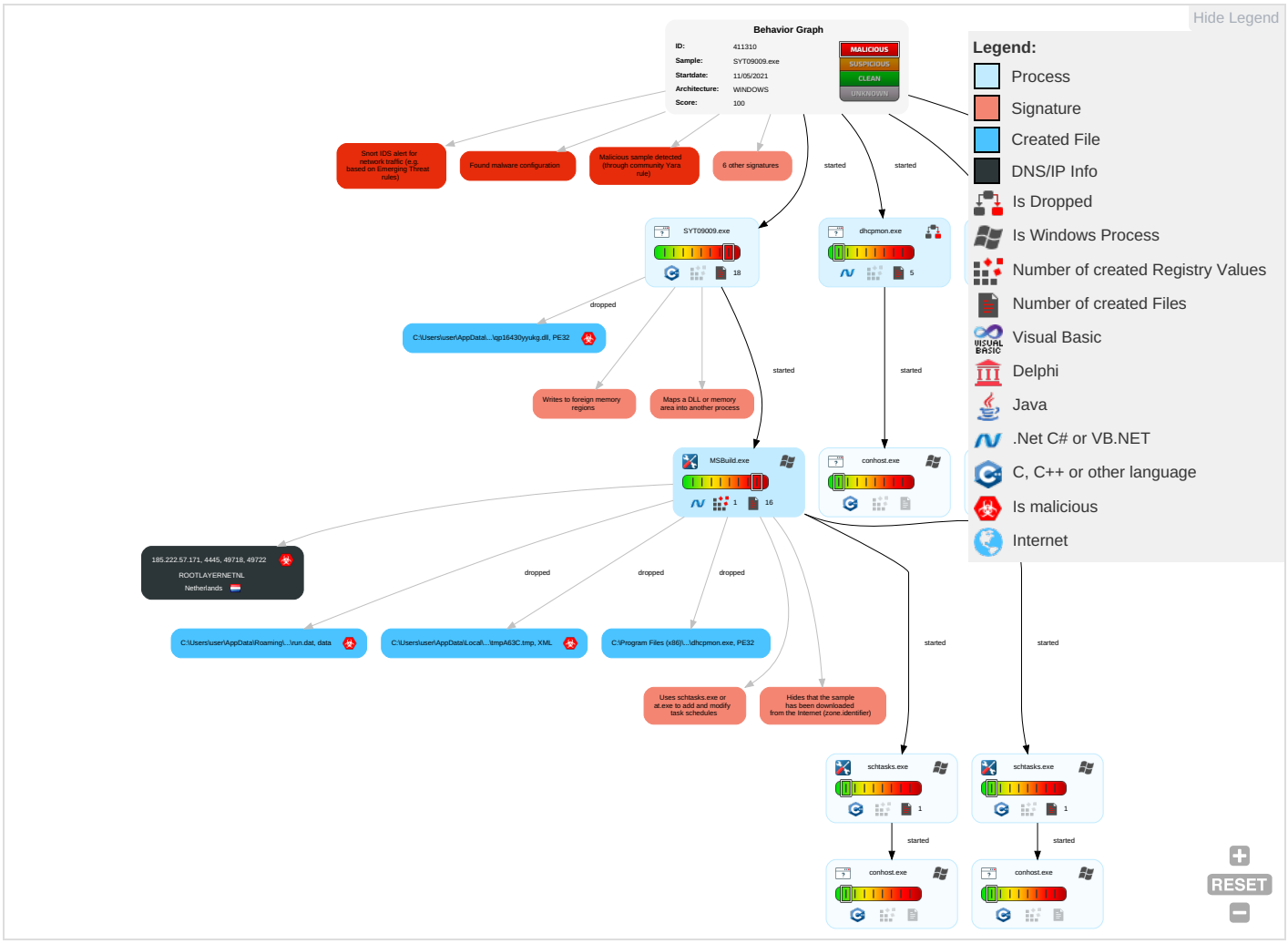
Detected Nanocore Rat

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	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Networ Commu
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

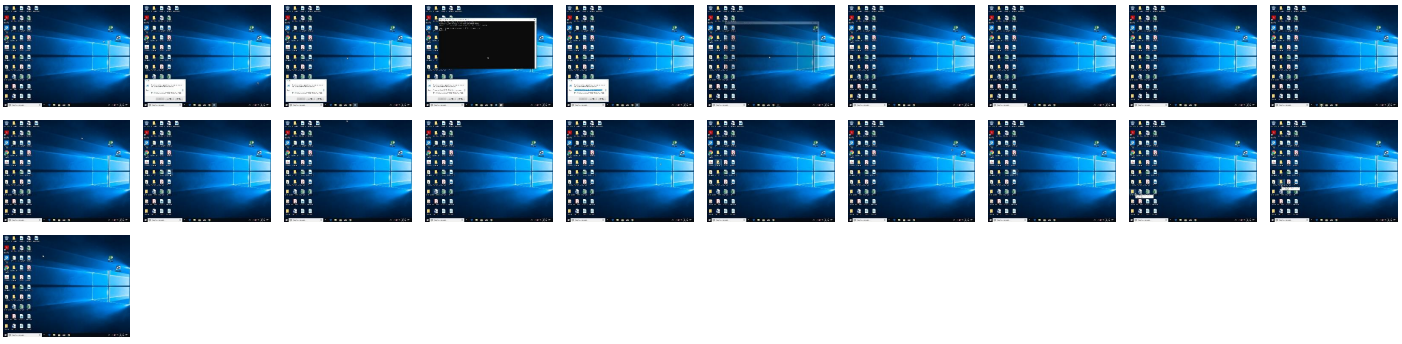
Behavior Graph



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
SYT09009.exe	38%	ReversingLabs	Win32.Trojan.SpyNoon	

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\nsg940D.tmp\qp16430yyukg.dll	11%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SYT09009.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.SYT09009.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
185.222.57.171	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

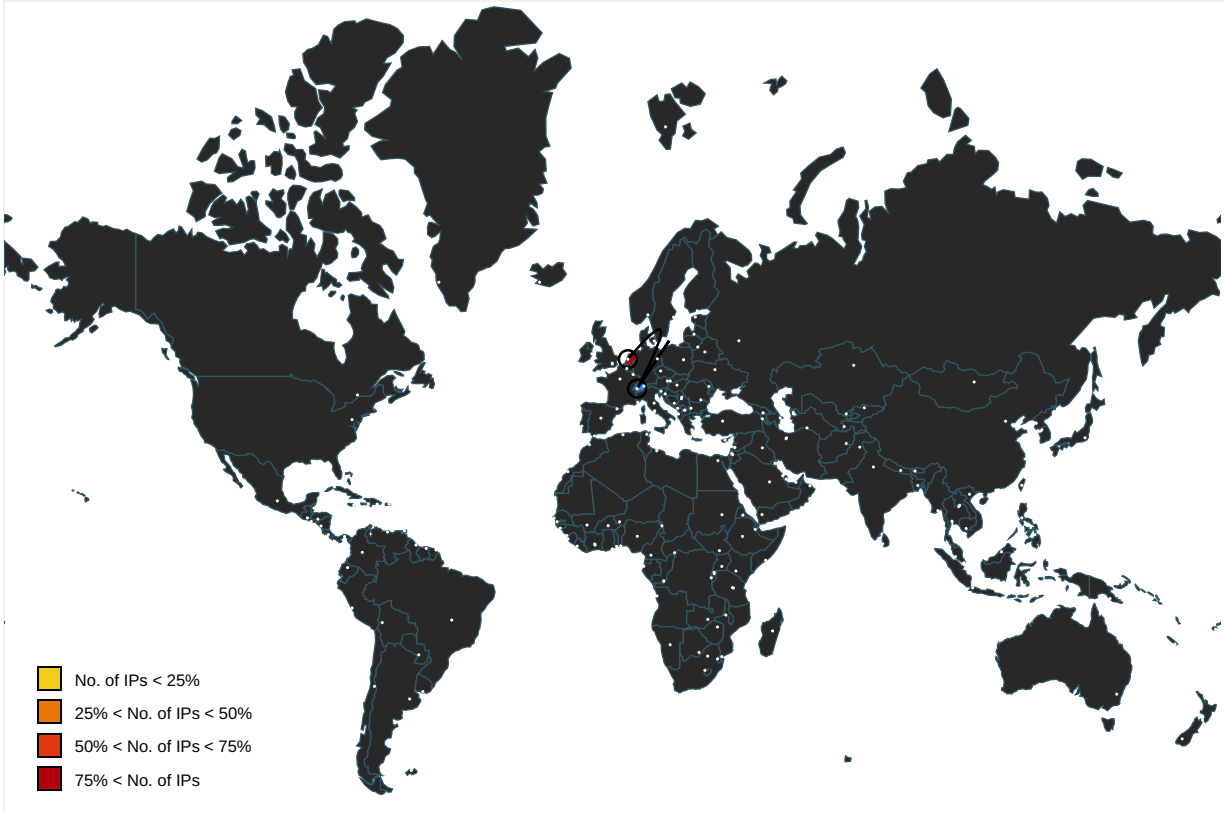
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
185.222.57.171	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	SYT09009.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	SYT09009.exe	false		high

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:	411310
Start date:	11.05.2021
Start time:	19:39:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SYT09009.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:	37
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@15/16@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26% (good quality ratio 24.6%) • Quality average: 82.3% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 52.255.188.83, 23.57.81.29, 92.122.145.220, 40.88.32.150, 23.57.80.111, 20.82.210.154, 92.122.213.194, 92.122.213.247, 2.20.143.16, 2.20.142.209, 51.103.5.186, 20.54.26.129, 52.155.217.156, 20.82.209.183 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/411310/sample/SYT09009.exe

Simulations

Behavior and APIs

Time	Type	Description
19:40:57	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
19:40:58	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)
19:40:58	API Interceptor	968x Sleep call for process: MSBuild.exe modified
19:41:00	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.222.57.171	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	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
	Order ConfirmationSANQAW12NC9W03.exe	Get hash	malicious	Browse	• 185.222.57.152

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
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: 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 • Filename: 7444478441.js, Detection: malicious, Browse
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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Entropy (8bit):	5.388715099859351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U2+gYhD5itZbgbe4MqJsGMe4M6:MLF20NaL32+g2OH4xvn4j
MD5:	88F0104DB9A3F9BC4F0FC3805F571B0D
SHA1:	CDD4F34385792F0CCE0A844F4ABB447C25AB4E73
SHA-256:	F6C11D3D078ED73F2640DA510E68DEEAA5F14F79CAE2E23A254B4E37C7D0230F
SHA-512:	04B977F63CAB8DE20EA7EFA9D4299C2E625D92FA6D54CA03EECD9F322E978326B353824F23BEC0E712083BDE0DBC5CC4EE90922137106B096050CA46A166DFE
Malicious:	false
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\5p0l53h9iyxojbq47	
Process:	C:\Users\user\Desktop\SYT09009.exe
File Type:	data
Category:	dropped
Size (bytes):	13829
Entropy (8bit):	7.988330917782456
Encrypted:	false
SSDEEP:	384:1GhUkGyqVQozym1urnHgmHpgRWkHmUmUiYPsAUTmx6b1Eu:1fVNyw4HVHp8WE/sAUTmx65Eu
MD5:	8552DD44F179CF07D797311847F7C2FE
SHA1:	C6F98C25CA2FF7B2274AFDC4C15962A01A6DABAD
SHA-256:	FE33D4505AB83ED038680604357D38D0AF928054D3C9FB1A17BB639A5007367A
SHA-512:	427B6D1276F1C73138283C533C06C708A17B7D96FC0F3DD67E28B1CF2F4647FA61266C58DA5D014F28049891688318C3CE81927CB77BD19CFD8F5627AFEC77FI
Malicious:	false
Preview:	^..kx.!_.6..{.v.7I:.T.....d...0D}...j.c...W.....|L.....F..5.eV.O*'T&u..4.....J..V[`b...[!(.....=.....-2.....$.O.+.u.}~..&.:Y#F...p_(+..A:dA.M...",.....^A.[n.*;.'.3....<ub.v...F'.[.g.\MN(.V.jI.v{..u.O.{..qjt..~}.2/<n.s,/.....q.....h...7.. pi...U.....I.W.....YZ9*&KP.....8aZ.Zm..fB?L~....?l4....~.....P.....B%..>.....;..d....?6.... "Q`...QJ.~.^]V...N... ..\|D56@...1.....X.0....rL.r5.E....6...$w4..8.fyz.....R.0.hk(..z$.:.NM.b_I^..._L.ef.....a...xj..g`sp...\|..E6....t.....I..:.....X.8H1*4...>=.....D....\dUV.mN...R.$.....|..g..[..e..~.....I0.. (.....:.....#.....T! ..b....>.JG.+A.U\`...]P.b'.R76;..}..0.....c.&..roG.y`mD8...%....zj_...'yz.....R;0.h.t.65.A.E...Q"..M..7..f..t...-.....n.6y..v...m.7.c<3....}.I..r.5.....p]..-T%Uf....vO.c..U.!.. a`Y....N.#...>....l.....^.....=.....B#...*....o9 ..D.$..6.*....~S..E..X(...ij.f....:7<.M... .,....u.%....f..K.n.....%e},...9-._

C:\Users\user\AppData\Local\Temp\al46nknojj	
Process:	C:\Users\user\Desktop\SYT09009.exe
File Type:	data
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	**7.9992611810929555**
Encrypted:	**true**
SSDEEP:	6144:WfOwF9z+53e7/1yzxQ63W9CgE4iB1fMMtD8Dq:QOMhEzWskiznkq
MD5:	C48006F5FF0B9B55937304AF196BCD29
SHA1:	4D1EA741919EACB5D19703006A93A5BB212AF905
SHA-256:	0A95E106ACB942AD49D9C4418BF3E0CCBC59CD27517BF35B7BC64AC3FE39240B
SHA-512:	C6DC55FD1F47BEAFC5E8355CF80AD5BF2FFB4810D33AA2212B9FF430787AD4D38E3A098D183616D253196692EA33D7ABCADEA47A5F85770C444669D0BC847CD
Malicious:	false
Preview:	]..0)....b.n.e;....7.....g.....,Ox.A.G.a.P.!\ye..d/.h.$..o..2.q"[..q....>.....am.....;.=..._6.....#..#z.d.E....d.p.....SRa1]..".FT.....\...9}....I..#....cx,...t_.....<`xL.....5..t.D.4Q.....T ..~..KY)~p7.Gbu#.};!.p..Z+LB../...y.=.....)+..P..R.H.1X;.....M.C..k.8....hr...x...)....H.bz._{..y...9.J....3-T. .L.Q.ca....B....~..'..... ..s.nc.!...Wn.7...8.....KZP..?.*R..(..g.9y..j B.r0"...&pS...]..2Xr ..\|.....4.N[?.o,u)..]....m.>..S.....>...<.}..P..i..k.....uI.....Y...zV....k../.G.i..G[z6.....h...5H.[.-..x..:.a.N.R5J.z.....&..M.....I..m.....:.....p...../E4m....Q... ...1....UO.'.....`....\|Bh<.5.W..<.ehc.....Z...t.....n0q..C.v.8...,...&.....c_..Y...gh].$.0....c.nf....<...{.C.]...VL.wA..W....5Qv....P.h!m.!..9JnreY)8....0.;...1A.L.4.{.L.....5.m.+q!..t[...m..k.#.'..Q...."/....."...1fkp.T....W....h.[b.....+...F..@$.*..0.....BT.T.....U.+.C..?....g.V^..R...ydq.....X6)z....a.jR..2.....M.yR...J.J..

C:\Users\user\AppData\Local\Temp\nsg940D.tmp\qp16430yyukg.dll	
Process:	C:\Users\user\Desktop\SYT09009.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.666261408441134
Encrypted:	false
SSDEEP:	48:q/i+k4fpTvQuPihxea/we6e+pI7Wfr8o4PjhNElXb:Eke9s/96e+prr8o2hAX
MD5:	ACB4B0447D4A7F16E56D26161C75BC84
SHA1:	5B2C4AE36591FA30777EE0621433DDC653BCB77C
SHA-256:	4A872908678E042C3112E6B0C0386C0718B33A452719CFEEB4E4ACCE7172C91E
SHA-512:	3C9C04D066D6E3FBE1860097EC2243AB07955D485C1A020FEF26C0A2566F64B698CB601571DEDCFED64A1201DBCD0D05480CD0E77A3A21F06673660D5B61D5C
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\nsg940D.tmp\qp16430yyukg.dll	
Antivirus:	• Antivirus: ReversingLabs, Detection: 11%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`..... .!..... ..... .....@..... ..L...!..... ..... ..... .....text..... ..`.rdata..... .....@..@.data...&....0.....@..... .....

C:\Users\user\AppData\Local\Temp\tmpA63C.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
Entropy (8bit):	5.136963558289723
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnc2xtn:cbk4oL600QydbQxIYODOLedq3ZLj
MD5:	AE766004C0D8792953BAFFFE8F6A2E3B
SHA1:	14B12F27543A401E2FE0AF8052E116CAB0032426
SHA-256:	1ABDD9B6A6B84E4BA1AF1282DC84CE276C59BA253F4C4AF05FEA498A4FD99540
SHA-512:	E530DA4A5D4336FC37838D0E93B5EB3804B9C489C71F6954A47FC81A4C655BB72EC493E109CF96E6E3617D7623AC80697AD3BBD5FFC6281BAFC8B34DCA5E65 7
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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpA9C7.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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhL
MD5:	74AACAE24C76D8BE7578A460BAE23521
SHA1:	523B694F22C1E962B7234BE9637DA09060CFB0C1
SHA-256:	2EFF42A56A82D1EB8E689FE73F5471B111FA17F1ECF72B90A731B59AFF691BFB
SHA-512:	5D715F8D14841552E280A9A5A5F749B23EEEBE713F7E95B288D921982800F2AB1FAAFDA67E420F28D882BF5904799E6BE62D4CAE451507FFB5EC3631B5D11FF6
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?. ..A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH }..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f. ..p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

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:b8:A
MD5:	D3220FBA2B0402A56F35209195959E3D
SHA1:	73A56FD2C595162AB8E9F61DEE5E062868F78A0A
SHA-256:	0971519E13E7EA981167C65746F6FA48B21F3E5091A79121E98D3A6995FD633B
SHA-512:	B4C2F2E5EB4EA7E9441ADBC90A37BF4260A5B249E70B8FC1C0020DF739F46F19EAD7615C1756F2E1BDEA4BBFEC0EBD90696657EB3CE3628B674C895ED7B0C473
Malicious:	**true**
Preview:	...^...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
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):	6.7295913886343195
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:	SYT09009.exe
File size:	555010
MD5:	fbfddfc110fd9d3775674447316de3d8
SHA1:	250149eebd54c774175cef2a09344cf429ca6f57
SHA256:	b98a4c0f84e431cbff5477f1e1ddfe1a93ba56775148cfca7f061f9beca0e48f
SHA512:	ffa4360b559cda6b7c1d5ec9cb0f89446be9f693a34c4bb35e6b8d4c26778d95e7139634cf6ba1896dc254c9bcc55fb171252c365ae678e59c8338a09261f842
SSDEEP:	6144:49X0GPoprRVuufOwF9z+53e7/1yzxQ63W9CgE4iB1fMMtD8Dbc:O0LrP/OMhEzWskiznkA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f...|.....H3.....@

File Icon

Icon Hash:	ae8cae8eb6aabe00

Static PE Info

General

Entrypoint:	0x403348
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

General

Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F8840A0D453h
push ebx
call 00007F8840A105B6h
cmp eax, ebx
je 00007F8840A0D449h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F8840A10532h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F8840A0D42Dh
push 0000000Bh
call 00007F8840A1058Ah
push 00000009h
call 00007F8840A10583h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F8840A10577h
cmp eax, ebx
je 00007F8840A0D451h
push 0000001Eh
call eax
test eax, eax
je 00007F8840A0D449h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx

Instruction
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x48ba8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x48ba8	0x48c00	False	0.0640470629296	data	4.76688901353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38340	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x7a368	0x25a8	data	English	United States
RT_ICON	0x7c910	0x10a8	data	English	United States
RT_ICON	0x7d9b8	0xea8	data	English	United States
RT_ICON	0x7e860	0x8a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x7f108	0x668	data	English	United States
RT_ICON	0x7f770	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x7fcd8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x80140	0x2e8	data	English	United States
RT_ICON	0x80428	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x80550	0x100	data	English	United States
RT_DIALOG	0x80650	0x11c	data	English	United States
RT_DIALOG	0x80770	0x60	data	English	United States
RT_GROUP_ICON	0x807d0	0x92	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x80868	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

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

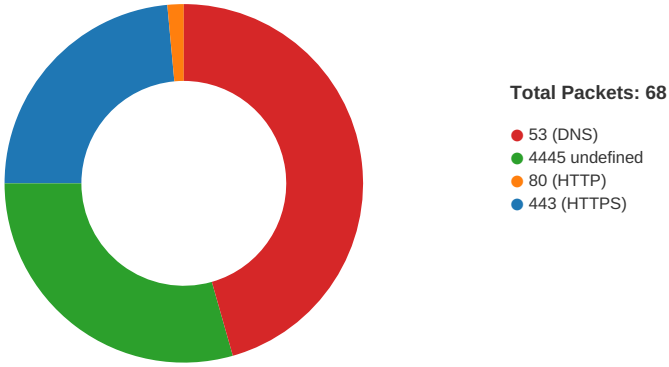
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/11/21-19:41:00.217795	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:07.017276	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:13.074122	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:17.376493	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:23.416228	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:30.481428	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:36.494819	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:42.950341	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:49.728010	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	4445	192.168.2.5	185.222.57.171
05/11/21-19:41:56.010318	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	4445	192.168.2.5	185.222.57.171

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/11/21-19:42:02.700606	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:08.910577	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:14.788279	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:20.775288	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:26.659939	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:32.535583	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:38.910159	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:44.786453	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:50.753969	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	4445	192.168.2.5	185.222.57.171
05/11/21-19:42:57.151446	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	4445	192.168.2.5	185.222.57.171

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 19:40:39.981837988 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:39.982028008 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525325060 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525486946 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525574923 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525631905 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525676966 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525705099 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525723934 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525751114 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525768995 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.525800943 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.572941065 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.572962999 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573002100 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573136091 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573510885 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573528051 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573539019 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573551893 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573559046 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573565006 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573609114 CEST	443	49703	131.253.33.200	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 19:40:44.573632956 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573751926 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573787928 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.573909998 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.573949099 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.574012041 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.574059010 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.574120998 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.574136972 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.574183941 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:44.574248075 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.574395895 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.751949072 CEST	443	49703	131.253.33.200	192.168.2.5
May 11, 2021 19:40:44.752115965 CEST	49703	443	192.168.2.5	131.253.33.200
May 11, 2021 19:40:46.702603102 CEST	49693	443	192.168.2.5	20.50.102.62
May 11, 2021 19:40:46.702687979 CEST	49696	80	192.168.2.5	93.184.220.29
May 11, 2021 19:40:46.702949047 CEST	49694	443	192.168.2.5	20.50.102.62
May 11, 2021 19:41:00.139692068 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.188246012 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.188344002 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.217794895 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.276120901 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.276194096 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.279598951 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.279716015 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.338560104 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.338622093 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.385493994 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.404017925 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.479083061 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.479147911 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.500022888 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.500044107 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.500060081 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.500076056 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.500087023 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.500097036 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.500159025 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.548785925 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548820019 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548832893 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548844099 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548860073 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548873901 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548886061 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548902035 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548913956 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.548979044 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.549019098 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.595504999 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595524073 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595540047 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595560074 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595577002 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595592022 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595597029 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.595607996 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595618963 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.595624924 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595638037 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.595640898 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595657110 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.595659971 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.595669031 CEST	4445	49718	185.222.57.171	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 19:41:00.595695019 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.598835945 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.598855972 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.598870993 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.598886967 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.598897934 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.598923922 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.598952055 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.602694035 CEST	49718	4445	192.168.2.5	185.222.57.171
May 11, 2021 19:41:00.642422915 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.642447948 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.642465115 CEST	4445	49718	185.222.57.171	192.168.2.5
May 11, 2021 19:41:00.642484903 CEST	4445	49718	185.222.57.171	192.168.2.5

UDP Packets

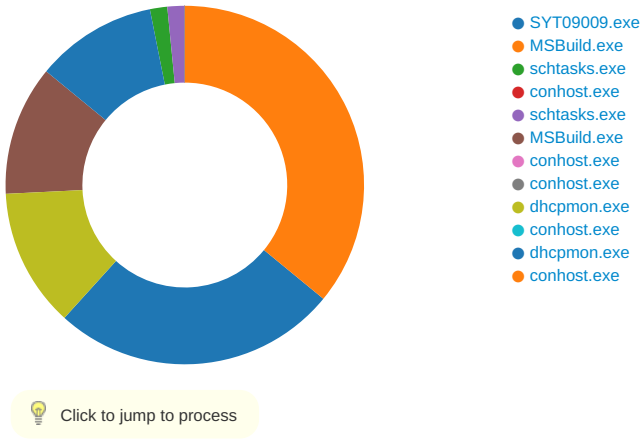
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 19:40:41.097431898 CEST	61733	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:41.148153067 CEST	53	61733	8.8.8.8	192.168.2.5
May 11, 2021 19:40:41.909591913 CEST	65447	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:41.959249020 CEST	53	65447	8.8.8.8	192.168.2.5
May 11, 2021 19:40:42.046721935 CEST	52441	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:42.105967999 CEST	53	52441	8.8.8.8	192.168.2.5
May 11, 2021 19:40:42.728183985 CEST	62176	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:42.785489082 CEST	53	62176	8.8.8.8	192.168.2.5
May 11, 2021 19:40:43.706080914 CEST	59596	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:43.754923105 CEST	53	59596	8.8.8.8	192.168.2.5
May 11, 2021 19:40:44.184880018 CEST	65296	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:44.247273922 CEST	53	65296	8.8.8.8	192.168.2.5
May 11, 2021 19:40:44.533559084 CEST	63183	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:44.582956076 CEST	53	63183	8.8.8.8	192.168.2.5
May 11, 2021 19:40:46.383810997 CEST	60151	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:46.436259031 CEST	53	60151	8.8.8.8	192.168.2.5
May 11, 2021 19:40:47.325426102 CEST	56969	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:47.384027958 CEST	53	56969	8.8.8.8	192.168.2.5
May 11, 2021 19:40:48.260334969 CEST	55161	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:48.311880112 CEST	53	55161	8.8.8.8	192.168.2.5
May 11, 2021 19:40:49.094321012 CEST	54757	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:49.144437075 CEST	53	54757	8.8.8.8	192.168.2.5
May 11, 2021 19:40:52.681729078 CEST	49992	53	192.168.2.5	8.8.8.8
May 11, 2021 19:40:52.733273029 CEST	53	49992	8.8.8.8	192.168.2.5
May 11, 2021 19:41:05.331192970 CEST	60075	53	192.168.2.5	8.8.8.8
May 11, 2021 19:41:05.394089937 CEST	53	60075	8.8.8.8	192.168.2.5
May 11, 2021 19:41:17.269723892 CEST	55016	53	192.168.2.5	8.8.8.8
May 11, 2021 19:41:17.326965094 CEST	53	55016	8.8.8.8	192.168.2.5
May 11, 2021 19:41:30.598397017 CEST	64345	53	192.168.2.5	8.8.8.8
May 11, 2021 19:41:30.652195930 CEST	53	64345	8.8.8.8	192.168.2.5
May 11, 2021 19:41:35.789753914 CEST	57128	53	192.168.2.5	8.8.8.8
May 11, 2021 19:41:35.848423958 CEST	53	57128	8.8.8.8	192.168.2.5
May 11, 2021 19:41:36.148536921 CEST	54791	53	192.168.2.5	8.8.8.8
May 11, 2021 19:41:36.205853939 CEST	53	54791	8.8.8.8	192.168.2.5
May 11, 2021 19:41:47.910130024 CEST	50463	53	192.168.2.5	8.8.8.8
May 11, 2021 19:41:47.980202913 CEST	53	50463	8.8.8.8	192.168.2.5
May 11, 2021 19:41:49.166731119 CEST	50394	53	192.168.2.5	8.8.8.8
May 11, 2021 19:41:49.225449085 CEST	53	50394	8.8.8.8	192.168.2.5
May 11, 2021 19:42:08.874237061 CEST	58530	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:08.995861053 CEST	53	58530	8.8.8.8	192.168.2.5
May 11, 2021 19:42:09.546247005 CEST	53813	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:09.662774086 CEST	53	53813	8.8.8.8	192.168.2.5
May 11, 2021 19:42:10.244744062 CEST	63732	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:10.305036068 CEST	53	63732	8.8.8.8	192.168.2.5
May 11, 2021 19:42:10.795542955 CEST	57344	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:10.853147984 CEST	53	57344	8.8.8.8	192.168.2.5
May 11, 2021 19:42:11.439920902 CEST	54450	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 19:42:11.499397993 CEST	53	54450	8.8.8.8	192.168.2.5
May 11, 2021 19:42:12.111586094 CEST	59261	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:12.168761969 CEST	53	59261	8.8.8.8	192.168.2.5
May 11, 2021 19:42:12.610980988 CEST	57151	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:12.668272018 CEST	53	57151	8.8.8.8	192.168.2.5
May 11, 2021 19:42:13.481811047 CEST	59413	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:13.539010048 CEST	53	59413	8.8.8.8	192.168.2.5
May 11, 2021 19:42:14.948851109 CEST	60516	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:15.012072086 CEST	53	60516	8.8.8.8	192.168.2.5
May 11, 2021 19:42:15.515224934 CEST	51649	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:15.566854954 CEST	53	51649	8.8.8.8	192.168.2.5
May 11, 2021 19:42:27.988873005 CEST	65086	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:28.056380987 CEST	53	65086	8.8.8.8	192.168.2.5
May 11, 2021 19:42:29.749424934 CEST	56432	53	192.168.2.5	8.8.8.8
May 11, 2021 19:42:29.812186003 CEST	53	56432	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SYT09009.exe PID: 4956 Parent PID: 5720

General

Start time:	19:40:51
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\SYT09009.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SYT09009.exe'
Imagebase:	0x400000
File size:	555010 bytes
MD5 hash:	FBFDDFC110FD9D3775674447316DE3D8
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: 00000000.00000002.251070693.0000000002450000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.251070693.0000000002450000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.251070693.0000000002450000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.251070693.0000000002450000.00000004.00000001.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	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsa939E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\5p0l53h9iyxojbq47	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\al46nknojj	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsg940D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA

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	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg940D.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	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg940D.tmp\qp16430yyukg.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa939E.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsg940D.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5p0l53h9iyxojbq47	unknown	13829	5e 83 14 6b 78 8e 21 5f a7 36 f9 83 7b e6 76 88 37 49 3a 8a 54 1a 05 8f a8 99 a2 0c f3 9d 1f 64 b7 d9 c5 90 30 44 7d 94 1c 0f 6a bc 63 f5 d9 05 57 9d aa 1b 8b ba be 7c 4c f0 ba c3 c0 92 cd 46 ac 1c 35 02 65 56 b5 4f 2a 27 54 26 75 dc fb 34 07 a5 fc ed ee c8 7f f6 a9 4a a9 d3 56 5b 60 62 d3 a0 af f8 5b 21 28 11 0a d4 11 aa dd 1e 1d f7 d2 cf dc 8e a5 d4 93 cc cf 3d 04 f5 f6 80 b7 ae d1 a2 f1 ab de f3 08 da cb 18 17 f0 03 c9 10 09 b2 0c 2d 32 f5 c6 05 9f 1a 17 24 f6 4f 8c 2b e4 b7 75 8c 7d 7e f8 8f 26 b9 3a 59 23 46 eb f0 92 f7 70 5f 28 2b d1 d8 41 3a 64 41 fa 4d 0e 0d c7 22 1f 2c 9e e7 84 e3 dc 1f 0d d4 a5 a6 f0 83 5e 41 d2 a1 5b 6e e3 b8 2a 3b c8 27 a0 33 b9 e0 d9 c2 3c 75 62 85 76 d5 ef 8a 87 b4 46 27 fc 5b 94 67 04 5c 4d 4e 28 13 56 09 6a 49 fa 76 7b 80	^..kx.!_.6..{.v.7I:.T..... .d....0D}...j.c...W.....|L... ...F..5.eV.O*'T&u..4.....J ..V[`b....[!(..... .=.....-2.. ....$.O.+..u.}~..&.:Y#F....p_ (+..A:dA.M...'',.....^A.. [n..*;.'.3....<ub.v.....F'.[. g.\MN(.V.jI.v{.	success or wait	1	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\al46nknojj	unknown	32768	5d f0 a1 d9 30 29 b1 c4 c9 be 89 62 d3 6e 93 65 3b 95 a9 b2 1c 37 d5 d5 f7 95 86 04 67 f2 d6 1c d8 8d 2c bb 4f 78 c1 41 bf 47 f3 61 af 50 a7 21 5c 79 65 96 81 64 2f 88 68 c9 24 11 aa 6f 0d f0 ac 32 c2 71 22 5b a0 c8 71 dc 9b ff c3 01 3e 8e 0e 01 cc 0a 61 6d e7 0d 8b bd a0 3b f9 3d 1d 15 ee 5f af 36 ba a2 16 00 15 11 23 ee e3 23 7a 9b 64 ec 45 06 fb 98 ee 64 c8 70 de fd b3 c4 e5 bc 53 52 61 31 5d 89 99 22 0f 0d 46 54 9e 0a b4 a8 1e be d0 5c be f9 9c 39 7d 8d dd 1d d4 6c 1e 16 23 09 0b 1e 94 63 78 2c 15 fa c5 74 5f ad b4 0a c1 07 c3 dc ae 3c 60 78 4c 2e 0e f3 01 ac 35 e9 f4 74 f9 44 b6 34 51 fb bb cb 96 c6 1b f1 06 54 1c ea 99 a2 7e f7 fd 4b 59 29 7e 70 37 a0 47 62 75 23 0f 7d 3b 21 fb 70 a3 b5 5a 2b 4c 42 89 82 2f 9b af c8 88 79 c3 3d 05 92 ee f5 93 13 89	]...0).....b.n.e;....7......g. ....,.Ox.A.G.a.P.!\ye..d/.h.$. .o...2.q"[..q.....>.....am.... .;.=..._.6......#..#z.d.E....d .p......SRa1]..".FT.......\.. .9}....l..#....cx,...t_........ <`xL.....5..t.D.4Q........T.. ..~..KY)~p7.Gbu#.};!.p..Z+ LB../....y.=.......	success or wait	7	405D51	WriteFile
C:\Users\user\AppData\Local\Temp\nsg940D.tmp\qp16430yyukg.dll	unknown	4608	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 bd 8d 9a 60 00 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 00 00 04 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE ..L......`...........!........	success or wait	1	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SYT09009.exe	unknown	512	success or wait	657	405D22	ReadFile
C:\Users\user\Desktop\SYT09009.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Users\user\Desktop\SYT09009.exe	unknown	4	success or wait	12	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\5p0l53h9iyxojbq47	unknown	13829	success or wait	1	100010CB	ReadFile
C:\Users\user\AppData\Local\Temp\al46nknojj	unknown	207872	success or wait	1	2442A34	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2440A58	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2440A58	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2440A58	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2440A58	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2440A58	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2440A58	ReadFile

Analysis Process: MSBuild.exe PID: 3332 Parent PID: 4956

General

Start time:	19:40:52
Start date:	11/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SYT09009.exe'
Imagebase:	0x4e0000
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, Description: unknown, Source: 00000001.00000003.258062190.0000000004043000.00000004.00000001.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	72B860AC	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	72B860AC	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	4D207A1	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	4D2089B	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	4D207A1	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	4D20B20	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA63C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4D20D1C	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	4D2089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA9C7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4D20D1C	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	4D207A1	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	4D207A1	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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4D2089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4D2089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4D2089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA63C.tmp	success or wait	1	BCBF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA9C7.tmp	success or wait	1	BCBF0E	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	f2 dc cb 5e ef 14 d9 48	...^...H	success or wait	1	4D20A53	WriteFile

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 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.....................@........... ....@.. ....@ ......99....@.................	success or wait	1	4D20B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA63C.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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	4D20A53	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	4D20A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA9C7.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	4D20A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	1	4D20A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426832	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%.....w.^.._.........B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	4D20A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	4D20A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	6	4D20A53	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72BB5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4D20A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	4D20A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	4D20A53	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	4D20C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 4320 Parent PID: 3332

General

Start time:	19:40:57
Start date:	11/05/2021
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\tmpA63C.tmp'
Imagebase:	0xbb0000
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\tmpA63C.tmp	unknown	2	success or wait	1	BBAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA63C.tmp	unknown	1321	success or wait	1	BBABD9	ReadFile

Analysis Process: conhost.exe PID: 5416 Parent PID: 4320

General

Start time:	19:40:57
Start date:	11/05/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 5840 Parent PID: 3332

General

Start time:	19:40:58
Start date:	11/05/2021
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\tmpA9C7.tmp'
Imagebase:	0xbb0000
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\tmpA9C7.tmp	unknown	2	success or wait	1	BBAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA9C7.tmp	unknown	1311	success or wait	1	BBABD9	ReadFile

Analysis Process: MSBuild.exe PID: 5868 Parent PID: 904

General

Start time:	19:40:58
Start date:	11/05/2021
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:	0xbd0000
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	72B860AC	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	72B860AC	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	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	12AA7A3	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	12AA7A3	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	12AA7A3	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	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.rsp	unknown	4096	success or wait	1	12AA7A3	ReadFile

Analysis Process: conhost.exe PID: 5880 Parent PID: 5840

General

Start time:	19:40:58
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: conhost.exe PID: 5872 Parent PID: 5868

General

Start time:	19:40:58
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: 4440 Parent PID: 904

General

Start time:	19:41:00
Start date:	11/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x740000
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	72B860AC	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	72B860AC	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	72B860AC	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	72B860AC	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	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7219DCB3	unknown
\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	7219DFAB	unknown
\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	7219DFAB	unknown
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\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..2,"Microsof	success or wait	1	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7219C1B7	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7219C1B7	unknown

Analysis Process: conhost.exe PID: 4684 Parent PID: 4440

General

Start time:	19:41:01
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6140 Parent PID: 3472

General

Start time:	19:41:05
Start date:	11/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x840000
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	72B860AC	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	72B860AC	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	72B860AC	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	72B860AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	112A897	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	112A897	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	112A897	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	112A897	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	112A897	ReadFile

Analysis Process: conhost.exe PID: 5876 Parent PID: 6140

General

Start time:	19:41:06
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis