ID: 343026
Sample Name: TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE
Cookbook: default.jbs
Time: 07:29:39
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report TNT SHIPMENT AWB_IMAGE CI_FROM…

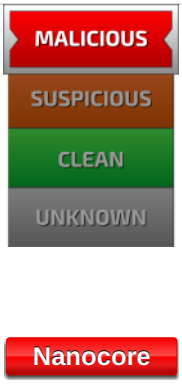
Overview

General Information

Sample Name:	TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____ _.EXE
Analysis ID:	343026
MD5:	d40d97b41a353b..
SHA1:	8e416c76489782..
SHA256:	23b46a12d6b6a7..
Tags:	EXE NanoCore

Most interesting Screenshot:

Detection



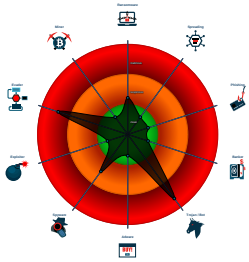
Nanocore

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 subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE (PID: 5816 cmdline: 'C:\Users\user\Desktop\TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE' MD5: D40D97B41A353BC42B0E7EBE451886D9)
  - conhost.exe (PID: 1372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 2204 cmdline: 'C:\Users\user\Desktop\TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE' MD5: D621FD77BD585874F9686D3A76462EF1)
    - schtasks.exe (PID: 7024 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp731A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6764 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp7609.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 6908 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6968 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 6796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 2480 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 6080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "91.193.75.155"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.656614146.0000000000AB0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.656614146.0000000000AB0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
00000001.00000002.656614146.0000000000AB0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.656614146.0000000000AB0000.00000004.00000001.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:$j: #=q
00000003.00000002.1047366764.0000000006580000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE.ab0000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.2.TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE.ab0000.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
1.2.TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE.ab0000.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE.ab0000.1.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q

Source	Rule	Description	Author	Strings
3.2.MSBuild.exe.6580000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 15 entries				

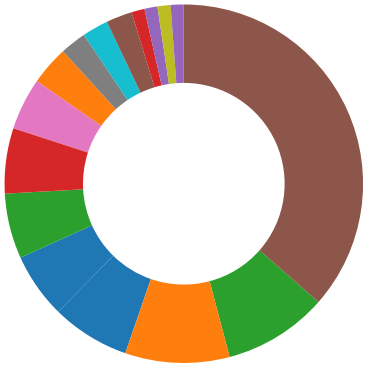
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

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

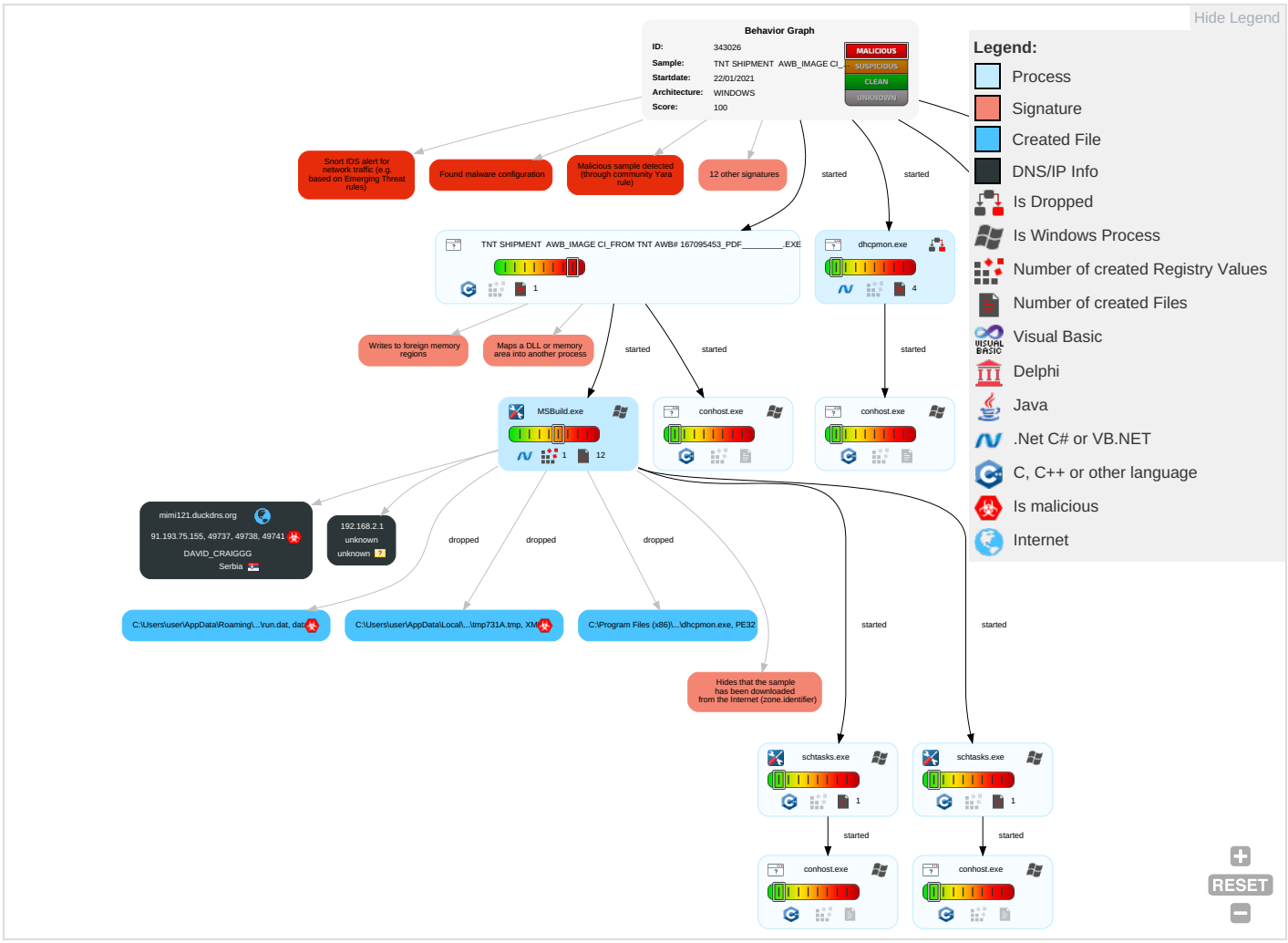
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Scheduled Task/Job 1 1	Scheduled Task/Job 1 1	Process Injection 2 1 2	Masquerading 2	Input Capture 1 1	System Time Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 3 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

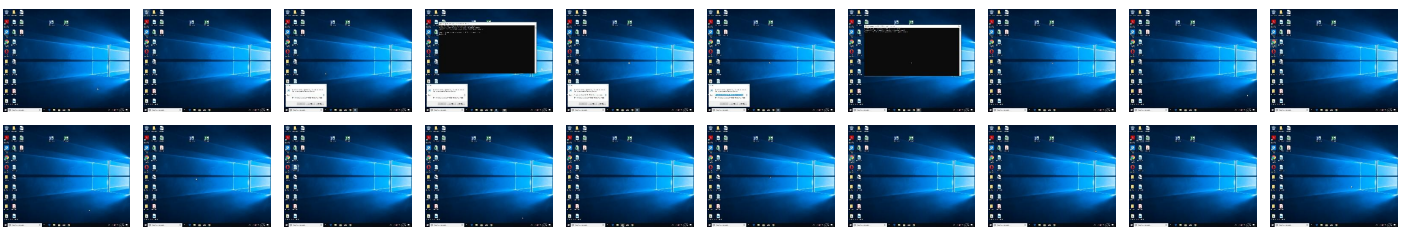
Behavior Graph



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
TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE	24%	Metadefender		Browse
TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE	59%	ReversingLabs	Win32.Spyware.Noon	
TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF__ _____.EXE.e30000.2.unpack	100%	Avira	HEUR/AGEN.1110392		Download File
3.2.MSBuild.exe.6580000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File

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

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mimi121.duckdns.org	91.193.75.155	true	true		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.193.75.155	unknown	Serbia		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343026
Start date:	22.01.2021
Start time:	07:29:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@16/11@26/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 57.2% (good quality ratio 52.8%) • Quality average: 81.9% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .EXE
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 51.11.168.160, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/343026/sample/TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE

Simulations

Behavior and APIs

Time	Type	Description
07:30:33	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
07:30:34	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe" s>$(Arg0)
07:30:34	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
07:30:34	API Interceptor	1546x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.193.75.155	file.exe	Get hash	malicious	Browse	
	Enquiry No ANS700_Pdf___.exe	Get hash	malicious	Browse	
	Enquiry No ANS700_Pdf___.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mimi121.duckdns.org	file.exe	Get hash	malicious	Browse	• 91.193.75.155
	Enquiry No ANS700_Pdf___.exe	Get hash	malicious	Browse	• 91.193.75.155
	Enquiry No ANS700_Pdf___.exe	Get hash	malicious	Browse	• 91.193.75.155

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	9A87wdxsuh.exe	Get hash	malicious	Browse	• 91.193.75.204
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	SecuriteInfo.com.Artemis1A5E2411DEA6.exe	Get hash	malicious	Browse	• 91.193.75.204
	Payment Invoice PDF.exe	Get hash	malicious	Browse	• 185.244.30.18
	New Doc 20211401#_our new price.exe	Get hash	malicious	Browse	• 91.193.75.243
	company profile.exe	Get hash	malicious	Browse	• 185.140.53.227
	NEWORDERrefno0992883jpg.exe	Get hash	malicious	Browse	• 185.140.53.253
	richiealvin.exe	Get hash	malicious	Browse	• 91.193.75.185
	Quotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	DHL Delivery Shipping Cargo. Pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	CompanyLicense.exe	Get hash	malicious	Browse	• 185.140.53.253
	Purchase Order 2094742424.exe	Get hash	malicious	Browse	• 185.244.30.132
	PURCHASE OREDER. PRINT. pdf.exe	Get hash	malicious	Browse	• 91.193.75.45
	PO.exe	Get hash	malicious	Browse	• 185.140.53.234
	SWIFT.exe	Get hash	malicious	Browse	• 185.140.53.154
	SecuriteInfo.com.BScope.Trojan-Dropper.Injector.exe	Get hash	malicious	Browse	• 185.140.53.234
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	Orden n.#U00ba STL21119, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Proof of Payment.exe	Get hash	malicious	Browse	• 185.244.30.51
	DxCHoDnNLn.exe	Get hash	malicious	Browse	• 185.140.53.202

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	New Order_PO#060317_007_Pdf_____.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.exe	Get hash	malicious	Browse	
	jCLiY7TCmD.exe	Get hash	malicious	Browse	
	WkyJ4e1mGH.exe	Get hash	malicious	Browse	
	Enquiry No ANS700_Pdf___.exe	Get hash	malicious	Browse	
	Enquiry No ANS700_Pdf___.exe	Get hash	malicious	Browse	
	P.I - AE-SA-10016 - SIG SHARBTLY INTERNATIONAL GROUP.exe	Get hash	malicious	Browse	
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	
	PAYMENT ADVICE.exe	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	
	Quotation Request-RFQ#2020-11-19.exe	Get hash	malicious	Browse	
	Api Details.exe	Get hash	malicious	Browse	
	BALANCE PAYMENT.exe	Get hash	malicious	Browse	
	5dj4XCE86M.exe	Get hash	malicious	Browse	
	z865yM9Ehy.exe	Get hash	malicious	Browse	
	EXPORT SHIPMENT CERTIFIED 2.exe	Get hash	malicious	Browse	
	4IZjnTicql.exe	Get hash	malicious	Browse	
	K1Rul7dwGf.exe	Get hash	malicious	Browse	
	14RP4w9CuA.exe	Get hash	malicious	Browse	
	Bx757nPqML.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	261728
Entropy (8bit):	6.1750840449797675
Encrypted:	false
SSDEEP:	3072:Mao0QHGUQWWimj9q/NLpj/WWqvAw2XpFU4rwOe4ubZSif02RFi/x2uv9FeP:boZTTWxxqVpqWVRXfr802biprVu
MD5:	D621FD77BD585874F9686D3A76462EF1
SHA1:	ABCAE05EE61EE6292003AABD8C80583FA49EDDA2
SHA-256:	2CA7CF7146FB8209CF3C6CECB1C5AA154C61E046DC07AFA05E8158F2C0DDE2F6
SHA-512:	2D85A81D708ECC8AF9A1273143C94DA84E632F1E595E22F54B867225105A1D0A44F918F0FAE6F1EB15ECF69D75B6F4616699776A16A2AA8B5282100FD15CA74C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: New Order_PO#060317_007_Pdf_____.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: jCLiY7TCmD.exe, Detection: malicious, Browse • Filename: WkyJ4e1mGH.exe, Detection: malicious, Browse • Filename: Enquiry No ANS700_Pdf___.exe, Detection: malicious, Browse • Filename: Enquiry No ANS700_Pdf___.exe, Detection: malicious, Browse • Filename: P.I - AE-SA-10016 - SIG SHARBTLY INTERNATIONAL GROUP.exe, Detection: malicious, Browse • Filename: Purchase Order 40,7045.exe, Detection: malicious, Browse • Filename: PAYMENT ADVICE.exe, Detection: malicious, Browse • Filename: Swift Copy.exe, Detection: malicious, Browse • Filename: Quotation Request-RFQ#2020-11-19.exe, Detection: malicious, Browse • Filename: Api Details.exe, Detection: malicious, Browse • Filename: BALANCE PAYMENT.exe, Detection: malicious, Browse • Filename: 5dj4XCE86M.exe, Detection: malicious, Browse • Filename: z865yM9Ehy.exe, Detection: malicious, Browse • Filename: EXPORT SHIPMENT CERTIFIED 2.exe, Detection: malicious, Browse • Filename: 4IZjnTicql.exe, Detection: malicious, Browse • Filename: K1Rul7dwGf.exe, Detection: malicious, Browse • Filename: 14RP4w9CuA.exe, Detection: malicious, Browse • Filename: Bx757nPqML.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....".....0..|...B.....n.... .....@.. ....`.....O.....>.....`>..... ....H.....text....z... ...|..... ..`.rsrc....>.....@...~.....@..@.relo c.....@..B.....P.....H.....8).....|.....*.{.....*v.(=....r...p({...-..+..}....*....0..%.....(....-..*....(z.....&..}.....*.*..... ...0..5.....(....-..*.-.r+..ps>...z.....i(z.....&..}.....*.*.....%.....>....(?...(....*N..(@....oA...(....*:...(B...(....*:...(C...(....**....(....*....0..G.....(.....*..(....-...}.....*.r...p(x...&.(v.....}... ...&..}.....*.*.....7.....0..f.....-.r7..ps>...z .....

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MSBuild.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	841
Entropy (8bit):	5.356220854328477
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoIvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHwvEHxDqHj
MD5:	486580834B084C92AE1F3866166C9C34
SHA1:	C8EB7E1CEF55A6C9EB931487E9AA4A2098AACEDF
SHA-256:	65C5B1213E371D449E2A239557A5F250FEA1D3473A1B5C4C5FF7492085F663FB
SHA-512:	2C54B638A52AA87F47CAB50859EFF98F07DA02993A596686B5617BA99E73ABFCD104F0F33209E24AFB32E66B4B8A225D4DB2CC79631540C21E7E8C4573DFD45
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1037
Entropy (8bit):	5.371216502395632
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7KvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHhAHKzvKvEHxD0
MD5:	C7F28B87C2CAD111D929CB9A0FF822F8
SHA1:	C2CF9E7A3F6EFD9000FE76EBE54E4E9AE5754267
SHA-256:	D1B02C20EACF464229AB063FA947A525E2ED7772259A8F70C7205DC13599EAE6
SHA-512:	E0F35874E02AB672CFF0553A0DA0864DAB14C05733D06395E4D0C9CDFC6F445E940310F8D01E3E1B28895F636DFBC1F510E103D1C46818400BA4E7371D8F254
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Temp\tmp731A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.137611098420233
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0moxtn:cbk4oL600QydbQxIYODOLedq3Zoj
MD5:	3E2B26ED8B75AE83A269595180E84EF6
SHA1:	D30A0335FCCE406BCA8BA5764288235E6192F608
SHA-256:	108BE30AEB8EB31C185A39A6726F26DACBC4E4124951C61A29ADE4B7038C71EA
SHA-512:	B6981C68FCB886CC8379A068B96931B9D4F5CC5AA9BDC467E36C4168FE6C5273A2A84D8850B12C11703EC03AC6B1F1950D1E669EFCB59FC2402CE4BBA9DC03D3
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp7609.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp7609.tmp	
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC08
MD5:	0D79388CEC6619D612C2088173BB6741
SHA1:	8A312E3198009C545D0CF3254572189D29A03EA7
SHA-256:	D7D423B23D932E306F3CCB2F7A984B7036A042C007A43FD655C6B57B960BB8DF
SHA-512:	53BB3E9263DFD746E7E8159466E220E6EC9D81E9D3F0E1D191E09CD511B7EB93B0BA65D13CE0C97C652ECD0F69BB991E6B1840F961BC65003C4DD7AA93EED 13
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.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\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:6VQ:6e
MD5:	80AF87D7D4711FE01B9BD93DEA99B562
SHA1:	85CA7BA9B80AEB0AF92FD9B3B394B1D86FE4C76C
SHA-256:	BD368AEEC8818B4106F481C92B7D242B079FAA718AD109E6D8779F613D1AB6FB
SHA-512:	5C55593F43C186EF0992AB60935877EA13EFD11310B98915414E50E2A5955B6ADEE4A79940C46C5CE838D2592BD1524728FB071C062A20BAA3208D8B479E6501
Malicious:	**true**
Preview:	...8...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.887726803973036
Encrypted:	false
SSDEEP:	3:oMty8WddSJ8:oMLW6C
MD5:	6ECAFC0490DAB08E4A288E0042B6B613
SHA1:	4A4529907588505FC65CC9933980CFE6E576B3D6
SHA-256:	DC5F76FBF44B3E6CDDC14EA9E5BB9B6BD3A955197FE13F33F7DDA7ECC08E79E0
SHA-512:	7DA2B02627A36C8199814C250A1FBD61A9C18E098F8D691C11D75044E7F51DBD52C31EC2E1EA8CDEE5077ADCCB8CD247266F191292DB661FE7EA1B613FC646 8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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):	298
Entropy (8bit):	4.943030742860529
Encrypted:	false
SSDEEP:	6:zx3M1tFAbQtU1R30qyMstwYVoRRZBXVN+J0fFdCsq2UTiMdH8stCal+n:zK13l30ZMt9BFN+QdCT2UftCM+
MD5:	6A9888952541A41F033EB114C24DC902
SHA1:	41903D7C8F31013C44572E09D97B9AAFBBCE77E6
SHA-256:	41A61D0084CD7884BEA1DF02ED9213CB8C83F4034F5C8156FC5B06D6A3E133CE
SHA-512:	E6AC898E67B4052375FDDFE9894B26D504A7827917BF3E02772CFF45C3FA7CC5E0EFFDC701D208E0DB89F05E42F195B1EC890F316BEE5CB8239AB45444DAA65E
Malicious:	false
Preview:	Microsoft (R) Build Engine version 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. 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 (console) Intel 80386, for MS Windows
Entropy (8bit):	6.925960933213739
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:	TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE
File size:	542720
MD5:	d40d97b41a353bc42b0e7ebe451886d9
SHA1:	8e416c76489782a32eade1b03bcd26dce3f19a82
SHA256:	23b46a12d6b6a703b8e588d24f3c0018cf749556b021b514b963587e7adaa25b
SHA512:	85d6c292351f8ff836337c9ace1c38e3f65cb15268d160c9f5e5f8f52ee7284834fa1c4a022bc58204664cf35ea348b802ff01d3f0d2b64b56b6bd4eb963c65d
SSDEEP:	6144:qJa6HhHoWXBuRPh6DnN+2gUFKLpGbNLpvlKK01gBxF8uUzeSg2ZDqnB8lRBYc:YlZYRsLN4cKLpGbNTjDF8u8JvKBkTj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....JH.*.).y.).y.).y..qy.).y..yy/).y..{y.).y..xy.).y.).yr).y.^.y.).y).xy.).y)..y.).y).zy.).yRich.).y.....PE..L...tt.`...

File Icon

Icon Hash:	70cccecececcec30

Static PE Info

General

Entrypoint:	0x404ad0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60097474 [Thu Jan 21 12:32:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	50cdb1b392e09bc322ca35e8f4935cd6

Entrypoint Preview

Instruction
call 00007FF2448D2107h
jmp 00007FF2448CA056h
and dword ptr [00420D24h], 00000000h
ret
push ebp
mov ebp, esp
push ecx
and dword ptr [ebp-04h], 00000000h
push 0041A29Ch
push 0041A2B0h
call dword ptr [0041A100h]
push eax
call dword ptr [0041A0D4h]
test eax, eax
je 00007FF2448CA224h
push 00000000h
lea ecx, dword ptr [ebp-04h]
push ecx
call eax
cmp eax, 7Ah
jne 00007FF2448CA217h
xor eax, eax
inc eax
leave
ret
xor eax, eax
leave
ret
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call dword ptr [0041A0E4h]
pop ebp
ret
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call dword ptr [0041A0F0h]
pop ebp
ret
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call dword ptr [0041A0E8h]
pop ebp
ret
push ebp

Instruction
mov ebp, esp
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call dword ptr [0041A0ECh]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 44h
lea eax, dword ptr [ebp-44h]
push eax
call dword ptr [0041A0FCh]
test byte ptr [ebp-18h], 00000001h
je 00007FF2448CA218h
movzx eax, word ptr [ebp-14h]
leave
ret
push 0000000Ah
pop eax
leave
ret
push ebp
mov ebp, esp
push ecx
push esi
mov esi, dword ptr [0041F368h]
test esi, esi
jns 00007FF2448CA245h
push 0041A29Ch
xor esi, esi
push 0041A2B0h
mov dword ptr [ebp-04h], esi
call dword ptr [00000000h]

Rich Headers

Programming Language:	• [LNK] VS2012 build 50727 • [RES] VS2012 build 50727 • [C] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1d564	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x327d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x55000	0xfdc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1cd18	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1a000	0x210	.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	0x18994	0x18a00	False	0.526233343909	data	6.49084256108	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x1a000	0x418e	0x4200	False	0.352095170455	data	4.70513234879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x2d60	0x1000	False	0.206787109375	data	2.47644845022	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x327d8	0x32800	False	0.384548073948	data	5.23228179627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x55000	0x123c	0x1400	False	0.6751953125	data	5.88808398568	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x22280	0x8f02	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	Chinese	Taiwan
RT_ICON	0x2b188	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	Chinese	Taiwan
RT_ICON	0x3b9b0	0x94a8	data	Chinese	Taiwan
RT_ICON	0x44e58	0x5488	data	Chinese	Taiwan
RT_ICON	0x4a2e0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 15794175, next used block 4294909696	Chinese	Taiwan
RT_ICON	0x4e508	0x25a8	data	Chinese	Taiwan
RT_ICON	0x50ab0	0x10a8	data	Chinese	Taiwan
RT_ICON	0x51b58	0x988	data	Chinese	Taiwan
RT_ICON	0x524e0	0x468	GLS_BINARY_LSB_FIRST	Chinese	Taiwan
RT_RCDATA	0x529d0	0x1e05	data	Chinese	Taiwan
RT_GROUP_ICON	0x52948	0x84	data	Chinese	Taiwan

Imports

DLL	Import
KERNEL32.dll	GetDiskFreeSpaceExA, ReleaseSemaphore, SearchPathW, GlobalGetAtomNameW, GetTickCount, TerminateJobObject, GetProcessHeap, LoadLibraryA, GetConsoleWindow, ReadConsoleInputA, PeekConsoleInputA, HeapAlloc, MoveFileExA, GetNumberOfConsoleInputEvents, SetEndOfFile, SetEnvironmentVariableA, CreateFileW, GetFileAttributesExW, CreateProcessA, GetExitCodeProcess, WaitForSingleObject, GetStringTypeW, EnumSystemLocalesEx, IsValidLocaleName, LCMapStringEx, GetUserDefaultLocaleName, GetLocaleInfoEx, CompareStringEx, GetDateFormatEx, GetTimeFormatEx, HeapSize, LoadLibraryW, OutputDebugStringW, WriteConsoleW, SetFilePointerEx, SetStdHandle, HeapReAlloc, FreeEnvironmentStringsW, GetEnvironmentStringsW, IsDebuggerPresent, IsProcessorFeaturePresent, EnterCriticalSection, LeaveCriticalSection, GetLastError, AreFileApisANSI, MultiByteToWideChar, EncodePointer, DecodePointer, InterlockedDecrement, ExitProcess, GetModuleHandleExW, GetProcAddress, GetCommandLineA, UnhandledExceptionFilter, SetUnhandledExceptionFilter, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, GetCurrentProcess, TerminateProcess, GetStartupInfoW, GetModuleHandleW, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, FatalAppExitA, HeapFree, Sleep, CloseHandle, FlushFileBuffers, GetStdHandle, WriteFile, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, GetFileType, InitOnceExecuteOnce, RtlUnwind, ReadFile, ReadConsoleW, SetFilePointer, DeleteFileW, MoveFileExW, GetModuleFileNameW, InterlockedExchange, FreeLibrary, LoadLibraryExW, SetConsoleCtrlHandler, InterlockedIncrement, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, SetLastError, GetCurrentThread, GetCurrentThreadId, GetModuleFileNameA, QueryPerformanceCounter, GetSystemTimeAsFileTime, GetTickCount64, SetConsoleMode
wsnmp32.dll	
CRYPT32.dll	CertGetEnhancedKeyUsage
ole32.dll	CreateAntiMoniker, OleSetAutoConvert, StringFromIID, HMETAFILE_UserUnmarshal, OleRegGetMiscStatus, RegisterDragDrop, CreateStreamOnHGlobal
SHELL32.dll	ShellExecuteA, FindExecutableA, SHGetFileInfo
pdh.dll	PdhOpenLogW, PdhBrowseCountersW
WINMM.dll	waveOutBreakLoop, midiInPrepareHeader, mmioGetInfo, joyGetPosEx, mixerMessage, waveInUnprepareHeader, mmioAdvance, mmioRenameA
USER32.dll	ShowWindow

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/22/21-07:30:35.963522	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	5090	192.168.2.4	91.193.75.155
01/22/21-07:30:43.444799	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	5090	192.168.2.4	91.193.75.155
01/22/21-07:30:51.244977	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	5090	192.168.2.4	91.193.75.155
01/22/21-07:30:58.286261	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:05.172412	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:12.170639	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:19.876213	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:26.508386	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:32.711233	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:38.673936	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:45.771730	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:51.904335	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	5090	192.168.2.4	91.193.75.155
01/22/21-07:31:59.176544	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:05.936635	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:13.035831	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:19.932310	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:26.960210	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:33.984764	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:41.028507	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:48.367382	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	5090	192.168.2.4	91.193.75.155
01/22/21-07:32:55.282856	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	5090	192.168.2.4	91.193.75.155
01/22/21-07:33:03.415066	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	5090	192.168.2.4	91.193.75.155
01/22/21-07:33:10.340730	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	5090	192.168.2.4	91.193.75.155
01/22/21-07:33:17.449587	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	5090	192.168.2.4	91.193.75.155
01/22/21-07:33:24.254331	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	5090	192.168.2.4	91.193.75.155
01/22/21-07:33:31.359828	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	5090	192.168.2.4	91.193.75.155

Network Port Distribution

Total Packets: 111

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 07:30:20.956803083 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.013168097 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.013232946 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.013360977 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.013421059 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.014260054 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.014326096 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.014359951 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.014389992 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.016556025 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.016612053 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.016670942 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.016699076 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.018930912 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.019045115 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.116935968 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.135690928 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.145804882 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.174531937 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.174561024 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.174685955 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.175635099 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.175720930 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.197650909 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.197694063 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.197871923 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.197925091 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.198873043 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.198899031 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.199003935 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.201628923 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.201677084 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.201725006 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.201759100 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.204328060 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.204370975 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.204435110 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.204461098 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.207010031 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.207043886 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.207102060 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.207128048 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.208759069 CET	443	49720	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.208794117 CET	443	49720	92.122.145.220	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 07:30:21.208839893 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.208884001 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.209450006 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.209716082 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.209759951 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.209803104 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.209829092 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.210047960 CET	443	49720	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.210091114 CET	443	49720	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.210115910 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.210144043 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.212443113 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.212486982 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.212543011 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.212560892 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.212590933 CET	443	49720	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.212629080 CET	443	49720	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.212651014 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.212696075 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.215147018 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.215195894 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.215233088 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.215244055 CET	443	49720	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.215260029 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.215308905 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.217942953 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.218010902 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.218050957 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.218101025 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.220582962 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.220626116 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.220695972 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.220732927 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.223262072 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.223306894 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.223351002 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.223386049 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.225946903 CET	443	49718	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.226032019 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.227494955 CET	49718	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.237905979 CET	49720	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.270323038 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.270376921 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.270437956 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.270474911 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.270895958 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.270937920 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.270975113 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.270996094 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.273289919 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.273345947 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.273397923 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.273418903 CET	49721	443	192.168.2.4	92.122.145.220
Jan 22, 2021 07:30:21.275707960 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.275753975 CET	443	49721	92.122.145.220	192.168.2.4
Jan 22, 2021 07:30:21.275809050 CET	49721	443	192.168.2.4	92.122.145.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 07:30:21.378611088 CET	49257	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:21.437596083 CET	53	49257	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:22.342644930 CET	62389	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:22.393596888 CET	53	62389	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 07:30:23.256931067 CET	49910	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:23.304858923 CET	53	49910	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:24.218707085 CET	55854	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:24.266788006 CET	53	55854	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:25.174165010 CET	64549	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:25.222306013 CET	53	64549	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:26.386390924 CET	63153	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:26.434209108 CET	53	63153	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:27.415808916 CET	52991	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:27.463816881 CET	53	52991	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:28.397255898 CET	53700	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:28.447101116 CET	53	53700	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:29.365123987 CET	51726	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:29.423111916 CET	53	51726	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:30.347744942 CET	56794	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:30.395719051 CET	53	56794	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:31.332916021 CET	56534	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:31.380970955 CET	53	56534	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:32.502029896 CET	56627	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:32.554056883 CET	53	56627	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:33.941205978 CET	56621	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:33.991930008 CET	53	56621	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:34.928697109 CET	63116	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:34.977129936 CET	53	63116	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:35.115108013 CET	64078	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:35.336199999 CET	53	64078	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:42.504307985 CET	64801	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:42.758469105 CET	53	64801	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:50.225294113 CET	61721	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:50.273416996 CET	53	61721	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:50.539695024 CET	51255	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:50.770622969 CET	53	51255	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:54.140110970 CET	61522	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:54.203713894 CET	53	61522	8.8.8.8	192.168.2.4
Jan 22, 2021 07:30:57.723223925 CET	52337	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:30:57.780884027 CET	53	52337	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:04.654083014 CET	55046	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:04.710472107 CET	53	55046	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:09.095591068 CET	49612	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:09.143719912 CET	53	49612	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:09.747498989 CET	49285	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:09.803611994 CET	53	49285	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:10.393574953 CET	50601	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:10.452713013 CET	53	50601	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:10.756057978 CET	60875	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:10.824704885 CET	53	60875	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:10.857202053 CET	56448	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:10.895068884 CET	59172	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:10.914729118 CET	53	56448	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:10.955908060 CET	53	59172	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:11.368948936 CET	62420	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:11.417228937 CET	53	62420	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:11.654519081 CET	60579	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:11.713551998 CET	53	60579	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:12.099128962 CET	50183	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:12.156215906 CET	53	50183	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:12.684833050 CET	61531	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:12.735503912 CET	53	61531	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:13.443432093 CET	49228	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:13.502599955 CET	53	49228	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:14.561983109 CET	59794	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:14.609958887 CET	53	59794	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:15.153989077 CET	55916	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:15.201973915 CET	53	55916	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 07:31:18.996299028 CET	52752	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:19.047084093 CET	53	52752	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:24.843041897 CET	60542	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:24.893831015 CET	53	60542	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:25.182035923 CET	60689	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:25.255044937 CET	53	60689	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:26.004311085 CET	64206	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:26.060651064 CET	53	64206	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:28.776148081 CET	50904	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:28.833760023 CET	53	50904	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:32.123198986 CET	57525	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:32.181315899 CET	53	57525	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:37.996712923 CET	53814	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:38.216588974 CET	53	53814	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:45.238523006 CET	53418	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:45.294686079 CET	53	53418	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:51.241583109 CET	62833	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:51.462378979 CET	53	62833	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:58.366811991 CET	59260	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:58.591681004 CET	53	59260	8.8.8.8	192.168.2.4
Jan 22, 2021 07:31:59.609966993 CET	49944	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:31:59.658224106 CET	53	49944	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:02.383984089 CET	63300	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:02.454840899 CET	53	63300	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:05.423141956 CET	61449	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:05.481987000 CET	53	61449	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:12.499536037 CET	51275	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:12.555836916 CET	53	51275	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:19.415810108 CET	63492	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:19.474915981 CET	53	63492	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:26.407856941 CET	58945	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:26.464147091 CET	53	58945	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:33.422535896 CET	60779	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:33.478782892 CET	53	60779	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:40.510041952 CET	64014	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:40.569143057 CET	53	64014	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:47.811078072 CET	57091	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:47.867594004 CET	53	57091	8.8.8.8	192.168.2.4
Jan 22, 2021 07:32:54.770771980 CET	55904	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:32:54.821542978 CET	53	55904	8.8.8.8	192.168.2.4
Jan 22, 2021 07:33:02.690608978 CET	52109	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:33:02.911175966 CET	53	52109	8.8.8.8	192.168.2.4
Jan 22, 2021 07:33:09.673223019 CET	54450	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:33:09.891906023 CET	53	54450	8.8.8.8	192.168.2.4
Jan 22, 2021 07:33:16.929156065 CET	49374	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:33:16.988557100 CET	53	49374	8.8.8.8	192.168.2.4
Jan 22, 2021 07:33:23.721820116 CET	50436	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:33:23.778325081 CET	53	50436	8.8.8.8	192.168.2.4
Jan 22, 2021 07:33:30.837969065 CET	62605	53	192.168.2.4	8.8.8.8
Jan 22, 2021 07:33:30.894315004 CET	53	62605	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 22, 2021 07:30:35.115108013 CET	192.168.2.4	8.8.8.8	0x8081	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:30:42.504307985 CET	192.168.2.4	8.8.8.8	0x8b76	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:30:50.539695024 CET	192.168.2.4	8.8.8.8	0x47bf	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:30:57.723223925 CET	192.168.2.4	8.8.8.8	0x18bc	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:04.654083014 CET	192.168.2.4	8.8.8.8	0x52f6	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:11.654519081 CET	192.168.2.4	8.8.8.8	0x98ce	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 22, 2021 07:31:18.996299028 CET	192.168.2.4	8.8.8.8	0xc52b	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:26.004311085 CET	192.168.2.4	8.8.8.8	0xb97b	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:32.123198986 CET	192.168.2.4	8.8.8.8	0xbbed	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:37.996712923 CET	192.168.2.4	8.8.8.8	0x2d2a	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:45.238523006 CET	192.168.2.4	8.8.8.8	0x9786	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:51.241583109 CET	192.168.2.4	8.8.8.8	0x7d59	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:58.366811991 CET	192.168.2.4	8.8.8.8	0x8811	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:05.423141956 CET	192.168.2.4	8.8.8.8	0xb1a0	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:12.499536037 CET	192.168.2.4	8.8.8.8	0xeb3e	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:19.415810108 CET	192.168.2.4	8.8.8.8	0x5110	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:26.407856941 CET	192.168.2.4	8.8.8.8	0x3361	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:33.422535896 CET	192.168.2.4	8.8.8.8	0x1b93	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:40.510041952 CET	192.168.2.4	8.8.8.8	0x6233	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:47.811078072 CET	192.168.2.4	8.8.8.8	0x202	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:54.770771980 CET	192.168.2.4	8.8.8.8	0xca19	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:02.690608978 CET	192.168.2.4	8.8.8.8	0xed44	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:09.673223019 CET	192.168.2.4	8.8.8.8	0x24d0	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:16.929156065 CET	192.168.2.4	8.8.8.8	0x74a0	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:23.721820116 CET	192.168.2.4	8.8.8.8	0x8bb5	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:30.837969065 CET	192.168.2.4	8.8.8.8	0x41bd	Standard query (0)	mimi121.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

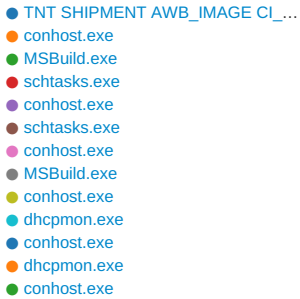
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 22, 2021 07:30:35.336199999 CET	8.8.8.8	192.168.2.4	0x8081	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:30:42.758469105 CET	8.8.8.8	192.168.2.4	0x8b76	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:30:50.770622969 CET	8.8.8.8	192.168.2.4	0x47bf	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:30:57.780884027 CET	8.8.8.8	192.168.2.4	0x18bc	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:04.710472107 CET	8.8.8.8	192.168.2.4	0x52f6	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:11.713551998 CET	8.8.8.8	192.168.2.4	0x98ce	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:19.047084093 CET	8.8.8.8	192.168.2.4	0xc52b	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:26.060651064 CET	8.8.8.8	192.168.2.4	0xb97b	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:32.181315899 CET	8.8.8.8	192.168.2.4	0xbbed	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:38.216588974 CET	8.8.8.8	192.168.2.4	0x2d2a	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)

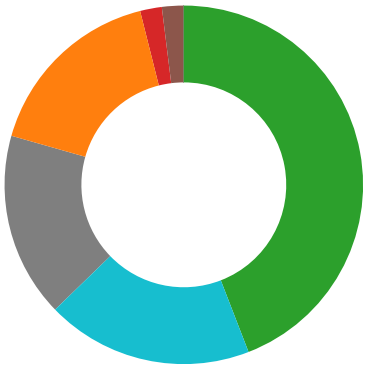
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 22, 2021 07:31:45.294686079 CET	8.8.8.8	192.168.2.4	0x9786	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:51.462378979 CET	8.8.8.8	192.168.2.4	0x7d59	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:31:58.591681004 CET	8.8.8.8	192.168.2.4	0x8811	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:05.481987000 CET	8.8.8.8	192.168.2.4	0xb1a0	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:12.555836916 CET	8.8.8.8	192.168.2.4	0xeb3e	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:19.474915981 CET	8.8.8.8	192.168.2.4	0x5110	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:26.464147091 CET	8.8.8.8	192.168.2.4	0x3361	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:33.478782892 CET	8.8.8.8	192.168.2.4	0x1b93	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:40.569143057 CET	8.8.8.8	192.168.2.4	0x6233	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:47.867594004 CET	8.8.8.8	192.168.2.4	0x202	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:32:54.821542978 CET	8.8.8.8	192.168.2.4	0xca19	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:02.911175966 CET	8.8.8.8	192.168.2.4	0xed44	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:09.891906023 CET	8.8.8.8	192.168.2.4	0x24d0	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:16.988557100 CET	8.8.8.8	192.168.2.4	0x74a0	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:23.778325081 CET	8.8.8.8	192.168.2.4	0x8bb5	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)
Jan 22, 2021 07:33:30.894315004 CET	8.8.8.8	192.168.2.4	0x41bd	No error (0)	mimi121.duckdns.org		91.193.75.155	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE PID: 5816 Parent PID: 5956

General

Start time:	07:30:27
Start date:	22/01/2021
Path:	C:\Users\user\Desktop\TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE'
Imagebase:	0xa50000
File size:	542720 bytes
MD5 hash:	D40D97B41A353BC42B0E7EBE451886D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.656614146.0000000000AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.656614146.0000000000AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.656614146.0000000000AB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.656614146.0000000000AB0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1372 Parent PID: 5816

General

Start time:	07:30:27
Start date:	22/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 2204 Parent PID: 5816

General

Start time:	07:30:29
Start date:	22/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095 453_PDF_____.EXE'
Imagebase:	0xad0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.1047366764.0000000006580000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.1047366764.0000000006580000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.1047366764.0000000006580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.1044661467.00000000040D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.1044661467.00000000040D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.1047272619.00000000064F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.1047272619.00000000064F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.1041355870.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.1041355870.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.1041355870.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	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	6D38CF06	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	6C1DBEFF	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	6C1D1E60	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	6C1DBEFF	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	6C1DDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp731A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1D7038	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	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp7609.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1D7038	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	6C1DBEFF	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	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	19	6C1D1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp731A.tmp	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7609.tmp	success or wait	1	6C1D6A95	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	ae ab 1a 38 9f be d8 48	...8...H	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 a1 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 22 01 0b 01 30 00 00 7c 03 00 00 42 00 00 00 00 00 00 6e 9a 03 00 00 20 00 00 00 a0 03 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 04 00 00 02 00 00 e8 d6 04 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... "...0..|...B......n.... ....@.. ....`................	success or wait	2	6C1DDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp731A.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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	6C1D1B4F	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 34 2e 30 2e 33 30 33 31 39 5c 4d 53 42 75 69 6c 64 2e 65 78 65	C:\Windows\Microsoft.NET \Frame work\v4.0.30319\MSBuild. exe	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7609.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	6C1D1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	7	6C1D1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D36CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D34D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D34D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	4096	success or wait	1	6D34D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	512	success or wait	1	6D34D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D365705	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WO W6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe	success or wait	1	6C1D646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 7024 Parent PID: 2204

General

Start time:	07:30:32
Start date:	22/01/2021
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\tmp731 A.tmp'
Imagebase:	0xc40000
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\tmp731A.tmp	unknown	2	success or wait	1	C4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp731A.tmp	unknown	1321	success or wait	1	C4ABD9	ReadFile

Analysis Process: conhost.exe PID: 5724 Parent PID: 7024

General

Start time:	07:30:32
Start date:	22/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6764 Parent PID: 2204

General

Start time:	07:30:33
Start date:	22/01/2021
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\tmp7609.tmp'
Imagebase:	0xc40000
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\tmp7609.tmp	unknown	2	success or wait	1	C4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7609.tmp	unknown	1311	success or wait	1	C4ABD9	ReadFile

Analysis Process: conhost.exe PID: 6708 Parent PID: 6764

General

Start time:	07:30:33
Start date:	22/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 6908 Parent PID: 968

General

Start time:	07:30:34
Start date:	22/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe 0
Imagebase:	0x10000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MSBuild.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C1D1B4F	WriteFile
\Device\ConDrv	unknown	161	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 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 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 76 65 72 73 69 6f 6e 20 34 2e 30 2e 33 30 33 31 39 2e 34 32 30 30 30 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 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 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6C1D1B4F	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	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MSBuild.exe.log	unknown	841	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6D69C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.rsp	unknown	4096	success or wait	1	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: 6964 Parent PID: 6908

General

Start time:	07:30:35
Start date:	22/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6968 Parent PID: 968

General

Start time:	07:30:35
Start date:	22/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xc70000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C1D1B4F	WriteFile
\Device\ConDrv	unknown	161	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 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 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 76 65 72 73 69 6f 6e 20 34 2e 30 2e 33 30 33 31 39 2e 34 32 30 30 30 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 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 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\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	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1037	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6D69C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: 6796 Parent PID: 6968

General

Start time:	07:30:35

Start date:	22/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 2480 Parent PID: 3424

General

Start time:	07:30:41
Start date:	22/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x10000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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	6D38CF06	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	6D38CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	161	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 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 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 76 65 72 73 69 6f 6e 20 34 2e 30 2e 33 30 33 31 39 2e 34 32 30 30 30 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 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 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6C1D1B4F	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	6C1D1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: 6080 Parent PID: 2480

General

Start time:	07:30:42
Start date:	22/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis