ID: 403691
Sample Name: Shipping Documents Original BL, Invoice & Pa.exe
Cookbook: default.jbs
Time: 10:29:25
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

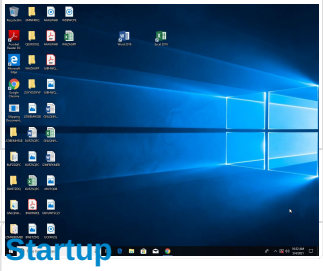
Analysis Report Shipping Documents Original BL, Invoi…

Overview

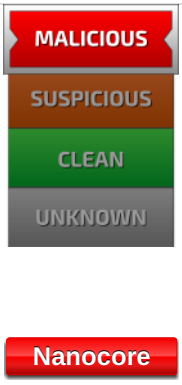
General Information

Sample Name:	Shipping Documents Original BL, Invoice & Pa.exe
Analysis ID:	403691
MD5:	b89d3e7dd6ee20..
SHA1:	d5a40ae65560da..
SHA256:	c2af0dcf4558a32..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



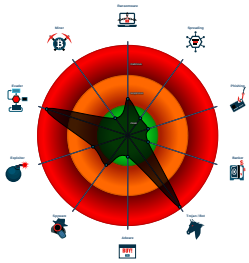
Nanocore

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

Signatures

- DLL reload attack detected
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- Shipping Documents Original BL, Invoice & Pa.exe (PID: 5936 cmdline: 'C:\Users\user\Desktop\Shipping Documents Original BL, Invoice & Pa.exe' MD5: B89D3E7DD6EE20A09506365497F6CC3A)
  - MSBuild.exe (PID: 5764 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
    - schtasks.exe (PID: 5792 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpF57E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 1680 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpF909.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 1556 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 1364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 980 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 4116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5728 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 4804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "692d457c-2b26-4af6-a5f8-088a1838",
  "Group": "Default",
  "Domain1": "",
  "Domain2": "172.93.166.26",
  "Port": 4090,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.673275544.0000000003DD9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x11fe0d:$x1: NanoCore.ClientPluginHost • 0x15282d:$x1: NanoCore.ClientPluginHost • 0x11fe4a:$x2: IClientNetworkHost • 0x15286a:$x2: IClientNetworkHost • 0x12397d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x15639d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.673275544.0000000003DD9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.673275544.0000000003DD9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x11fb75:$a: NanoCore • 0x11fb85:$a: NanoCore • 0x11fdb9:$a: NanoCore • 0x11fdcd:$a: NanoCore • 0x11fe0d:$a: NanoCore • 0x152595:$a: NanoCore • 0x1525a5:$a: NanoCore • 0x1527d9:$a: NanoCore • 0x1527ed:$a: NanoCore • 0x15282d:$a: NanoCore • 0x11fbd4:$b: ClientPlugin • 0x11fdd6:$b: ClientPlugin • 0x11fe16:$b: ClientPlugin • 0x1525f4:$b: ClientPlugin • 0x1527f6:$b: ClientPlugin • 0x152836:$b: ClientPlugin • 0x11fcfb:$c: ProjectData • 0x15271b:$c: ProjectData • 0x272bb6:$c: ProjectData • 0x2f4bd6:$c: ProjectData • 0x120702:$d: DESCrypto
00000000.00000002.670633702.0000000002E4C000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: Shipping Documents Original BL, Invoice & Pa.exe PID: 5936	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x30800:$x1: NanoCore.ClientPluginHost • 0x4f2a6:$x1: NanoCore.ClientPluginHost • 0x30861:$x2: IClientNetworkHost • 0x4f307:$x2: IClientNetworkHost • 0x35c66:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x43bd8:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x5470c:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x6267e:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Shipping Documents Original BL, Invoice & Pa.exe.3ee8c80.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Shipping Documents Original BL, Invoice & Pa.exe.3ee8c80.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.Shipping Documents Original BL, Invoice & Pa.exe.3ee8c80.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Shipping Documents Original BL, Invoice & Pa.exe.3ee8c80.3.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:$j: #=q
0.2.Shipping Documents Original BL, Invoice & Pa.exe.3ee8c80.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x42bad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x42bea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4671d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 2 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: System File Execution Location Anomaly

Sigma detected: Possible Applocker Bypass

Persistence and Installation Behavior:

Sigma detected: Scheduled temp file as task from temp location

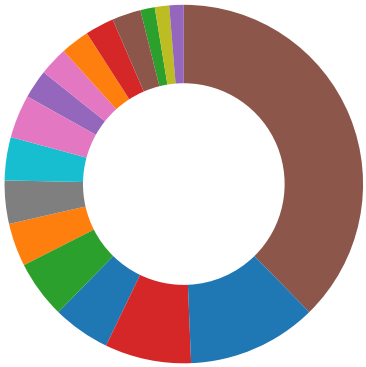
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Persistence and Installation Behavior:

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

DLL reload attack detected

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

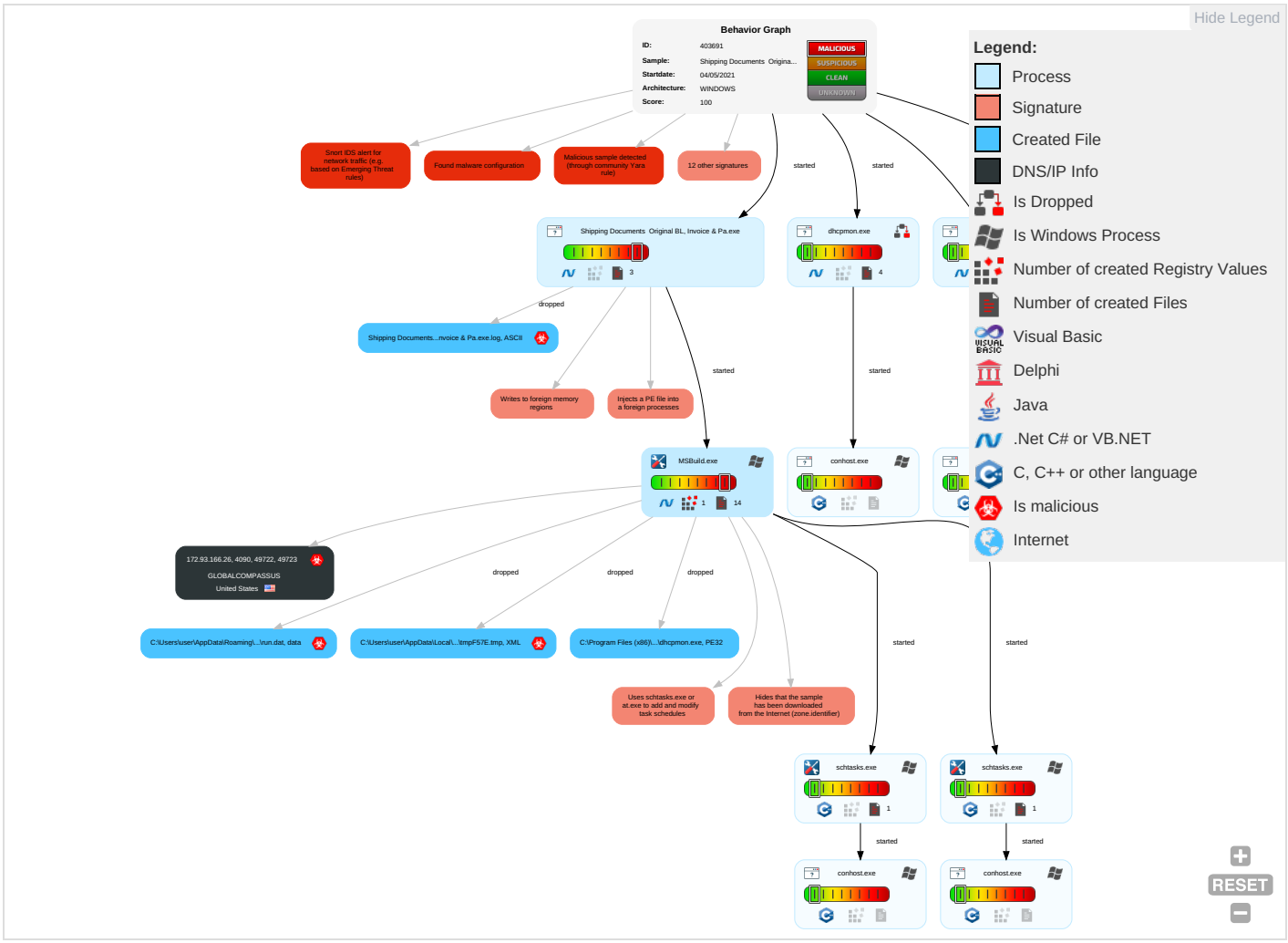
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1 1	Process Injection 2 1 1	Masquerading 2	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job 1 1	DLL Side-Loading 1	Scheduled Task/Job 1 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Remote Access Software 1	Ex Re Ca
Domain Accounts	Native API 1	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SII Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pr

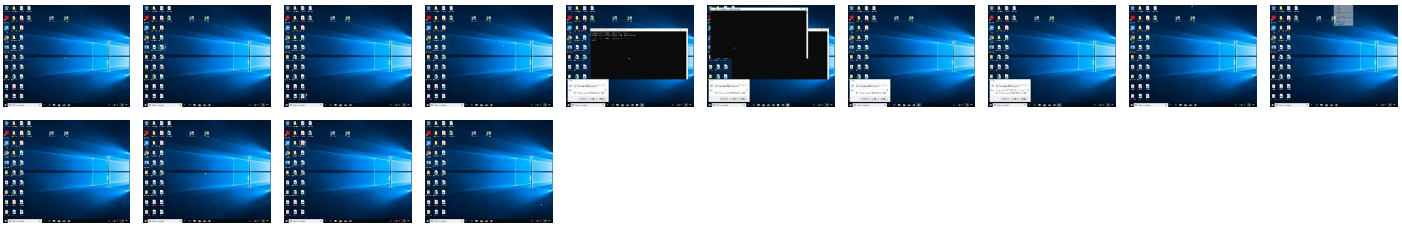
Behavior Graph



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
Shipping Documents Original BL, Invoice & Pa.exe	6%	ReversingLabs		
Shipping Documents Original BL, Invoice & Pa.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

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.monot.	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.goodfont.co.kr0l	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krr	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/type	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr.	0%	Avira URL Cloud	safe	
http://www.churchsw.org/repository/Bibles/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kra-d	0%	Avira URL Cloud	safe	
172.93.166.26	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krK	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kre	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sandoll.co.krcom	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.churchsw.org/church-projector-project	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

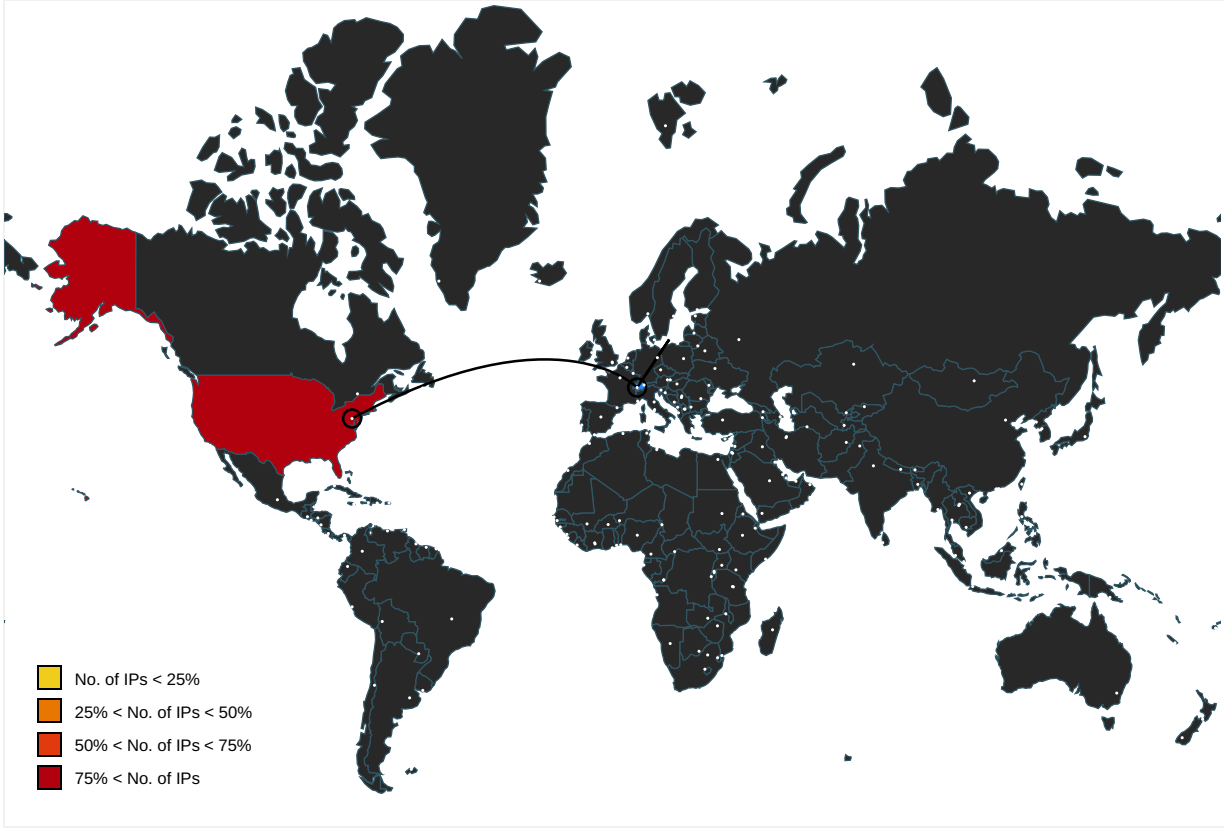
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monot.	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.660037136.0000000006025000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.670478696.0000000001520000.00000004.00000040.sdmp	false		high
http://www.fontbureau.com/designersG	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr0I	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.652728425.0000000005FFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krr	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.652728425.0000000005FFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.ascendercorp.com/type	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.654396019.0000000005FFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr.	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.652728425.0000000005FFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.churchsw.org/repository/Bibles/	Shipping Documents Original BL, Invoice & Pa.exe	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kra-d	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.652728425.0000000005FFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.krK	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.652728425.0000000005FFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kre	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.652728425.0000000005FFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.670633702.0000000002E4C000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.659032488.0000000005FFB000.00000004.00000001.sdmp, Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.658535409.0000000005FFC000.00000004.00000001.sdmp, Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.656756517.0000000005FFC000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krcom	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.652728425.0000000005FFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.como	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.670478696.0000000001520000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnt	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.653276119.0000000006005000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false		high
http://www.churchsw.org/church-projector-project	Shipping Documents Original BL, Invoice & Pa.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html8	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.656074649.0000000005FFC000.00000004.00000001.sdmp	false		high
http://www.fonts.com	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.651499309.000000000600B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.657239356.0000000005FFC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.670534502.0000000002DD1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000002.676141960.0000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	Shipping Documents Original BL, Invoice & Pa.exe, 00000000.00000003.655221857.0000000005FFC000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.93.166.26	unknown	United States		22653	GLOBALCOMPASSUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403691
Start date:	04.05.2021
Start time:	10:29:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping Documents Original BL, Invoice & Pa.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/14@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 5.2% (good quality ratio 4.5%) • Quality average: 38.1% • Quality standard deviation: 20%
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 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 52.147.198.201, 168.61.161.212 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:30:22	API Interceptor	1x Sleep call for process: Shipping Documents Original BL, Invoice & Pa.exe modified
10:30:28	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe" s>$(Arg0)
10:30:28	API Interceptor	970x Sleep call for process: MSBuild.exe modified
10:30:30	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
10:30:31	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GLOBALCOMPASSUS	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 69.61.16.162
	pieChart2.exe	Get hash	malicious	Browse	• 142.202.205.89
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKeep.htm	Get hash	malicious	Browse	• 69.61.20.27
	parcel_images.exe	Get hash	malicious	Browse	• 69.61.59.215
	a4588f57322665c795bdf720abc23ffc.exe	Get hash	malicious	Browse	• 69.61.52.111
	Mf1iDAE6bE.exe	Get hash	malicious	Browse	• 69.61.52.111
	Buchung.doc	Get hash	malicious	Browse	• 69.61.42.251
	Buchung.doc	Get hash	malicious	Browse	• 69.61.42.251

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Buchung.doc	Get hash	malicious	Browse	• 69.61.42.251
	P64.exe	Get hash	malicious	Browse	• 69.61.38.132
	http://v.ht/v6GD	Get hash	malicious	Browse	• 69.61.26.121

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	
	SN-346.exe	Get hash	malicious	Browse	
	insurance certificate , BL.exe	Get hash	malicious	Browse	
	E5ew8dBzdN.exe	Get hash	malicious	Browse	
	kHisp6Vo3M.exe	Get hash	malicious	Browse	
	aVzenPkPSm.exe	Get hash	malicious	Browse	
	GT42536.scr.exe	Get hash	malicious	Browse	
	NEWPO-243769001.exe	Get hash	malicious	Browse	
	Purchase Order-877.exe	Get hash	malicious	Browse	
	W29wJd8rZ5.exe	Get hash	malicious	Browse	
	INV#6534524.exe	Get hash	malicious	Browse	
	xWwkCdgUxd.exe	Get hash	malicious	Browse	
	t5R60D503x.exe	Get hash	malicious	Browse	
	GT_0397337_03987638BNG.exe	Get hash	malicious	Browse	
	CCF20032021_0003.exe	Get hash	malicious	Browse	
	1PH37n4Gva.exe	Get hash	malicious	Browse	
	E0029876556_209876689.exe	Get hash	malicious	Browse	
	BGD_03987365_0398736DSC.exe	Get hash	malicious	Browse	
	1XCQ1u2Q59.exe	Get hash	malicious	Browse	
	ROdimkVzMC9cn4X.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%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: SN-346.exe, Detection: malicious, Browse • Filename: insurance certificate , BL.exe, Detection: malicious, Browse • Filename: E5ew8dBzdN.exe, Detection: malicious, Browse • Filename: kHisp6Vo3M.exe, Detection: malicious, Browse • Filename: aVzenPkPSm.exe, Detection: malicious, Browse • Filename: GT42536.scr.exe, Detection: malicious, Browse • Filename: NEWPO-243769001.exe, Detection: malicious, Browse • Filename: Purchase Order-877.exe, Detection: malicious, Browse • Filename: W29wJd8rZ5.exe, Detection: malicious, Browse • Filename: INV#6534524.exe, Detection: malicious, Browse • Filename: xWwkCdgUxd.exe, Detection: malicious, Browse • Filename: t5R60D503x.exe, Detection: malicious, Browse • Filename: GT_0397337_03987638BNG.exe, Detection: malicious, Browse • Filename: CCF20032021_0003.exe, Detection: malicious, Browse • Filename: 1PH37n4Gva.exe, Detection: malicious, Browse • Filename: E0029876556_209876689.exe, Detection: malicious, Browse • Filename: BGD_03987365_0398736DSC.exe, Detection: malicious, Browse • Filename: 1XCQ1u2Q59.exe, Detection: malicious, Browse • Filename: RO dimkVzMC9cn4X.exe, Detection: malicious, Browse
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
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
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\Shipping Documents Original BL, Invoice & Pa.exe.log	
Process:	C:\Users\user\Desktop\Shipping Documents Original BL, Invoice & Pa.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Category:	modified
Size (bytes):	1037
Entropy (8bit):	5.371216502395632
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7KvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHhAHKzvKvEHxD0
MD5:	C7F28B87C2CAD111D929CB9A0FF822F8
SHA1:	C2CF9E7A3F6EFD9000FE76EBE54E4E9AE5754267
SHA-256:	D1B02C20EACF464229AB063FA947A525E2ED7772259A8F70C7205DC13599EAE6
SHA-512:	E0F35874E02AB672CFF0553A0DA0864DAB14C05733D06395E4D0C9CDFC6F445E940310F8D01E3E1B28895F636DFBC1F510E103D1C46818400BA4E7371D8F254E
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\tmpF57E.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\tmpF909.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):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.109925499344649

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Encrypted:	false
SSDEEP:	48:IkXEUg6ikXEUg6ikXEUg6ikXEUg6ikXEUg6ikXEUg6ikXEUg6ikXEUg6Z:06y6y6y6y6y6y6y6Z
MD5:	B75C7318FEA570C38EC018F2E906702F
SHA1:	05B91D7DFF32A62966BA7C58BD42C60E70C8C54B
SHA-256:	828C3ECDFC1F82F6D579A4FA1D140D1AFF98A986D5B10A5B94BD0EC19C8D3BB6
SHA-512:	75FF9ACA7EF41FE7ED8D9FAD0CB11A68F002AF79A3D7AB79314D473D6F5A30B557A7D9FD470B6F3FF75F690D70446FC5286CC5015DBF8AFCF73FBE725EEEC 0C
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ..JR<..e.8....z...O......f..m.PQ>Y...}.....K.,Kl..G.....qA..#.w.&..7m..B.I.....in..<5J....z).H?....6..*2Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ..JR<..e.8....z...O......f..m.PQ>Y...}.....K.,Kl..G.....qA..#.w.&..7m..B.I.....in..<5J....z).H?....6..*2Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ..JR<..e.8....z...O......f..m.PQ>Y...}.....K.,Kl..G.....qA..#.w.&..7m..B.I.....in..<5J....z).H?....6..*2Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ..JR<..e.8....z...O......f..m.PQ>Y...}.....K.,Kl..G.....qA..#.w.&..7m..B.I.....in..<5J....z).H?....6..*2Gj.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:Pcn:0n
MD5:	DE7A67A3040AC701DA32B2080CBB7529
SHA1:	8F9F4EC574D3C30BBD666DF38D513CA1E9B234FC
SHA-256:	0B977E561E1A854A31E242E5E68D143D677A9EB875A5D5FB49C30C547DF2D6FD
SHA-512:	B4ACF0DBD66C30C84B85C656B6A83AF8A088A74679CE26196698BF38271AF78F2BC9F002647171B1C298B12230EF69BA6199BD2C33256C44E67E121A5E4013E
Malicious:	**true**
Preview:	.v^....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44 F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	315512
Entropy (8bit):	**7.999402922203056**
Encrypted:	**true**
SSDEEP:	6144:m8aeVE5MlgWfxwY/8uvJYRDMVpXUhXShjVd/WNXlMjwmZ/zVR5X7HZEKiMIqrjG:mfwiMdxwYEYyWVjVpW7mZBDCgrjG
MD5:	787AEB1604A638B138739ED060141E9D
SHA1:	A2D0680883E8C6FF3DDE0A177263B03E7644D4AA
SHA-256:	DCCB67209560E2E27A4F284CD7E412926303ABD4E77927F9A1BAF8B0B8994B45
SHA-512:	9E49E851465F07ABA6AB44AD6B7561004AD61C4794FE167C6C724994159714AF8D2AC8ECCCE128F84BC6A7607BA05CD891CFD2C9EDE9D9EFA860346F600436 E
Malicious:	false
Preview:	..f# ....)1*.....5....;.T..u.. .3.Xd... ....u(..._.V.{L..Y.8....~...S79.f0V...=.}...SJg|.lh.J..^Ge.........3h?n..:..r....,o."a.I....\..0Z.D..........^....[..f.I....@/_..".5+...I...J`./s..p-.....c..?...*.. .&.....>.Ye$=.pG.....9D...'7.w.a.[3.d.-..V..]..B.b.zA?..M..3...%A....K5@.. j.U.h.B....'...0."..u.V...d..c,r"..@9.9.>..cDgP~d9..St...{..24.s.'.....9.D..P4.....I...G..G5......u.-2...z1[.....C..n.6.!..'.%@&.l4..P..rc+vq..C5B.b*..j.W,..T..z......)BX4...>A.*~#..A....8..B....5....w....GC..........y......7...?.T.....!.....7A.........C.3......A.....hC..5'..42..zS.*2.m7....A.'/.R..X....}e...>........}...n.A...4..?.P.l..n.0.I`...".d1.(e\|..f.....i.9.#...n..+..l....Xz.q...6".Hl...+...1^pgs...%.FR.T....(...=.rHX.d.9%...?..f?.Q.yi.D9/>....V..5......q...nP'...S.Y.....pu.!..-..\..\|/....V.......NX....../.8..V.0.5`m$.{b..lw.K.3-..C3...-.2.Qb.....o...6z....`H...(..o.ag.-7../F..RoI..O#.u|.U.@....$;.....s.~.M...j?...q#.l..y..M.[../.....=T.......5HX.QJ...

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
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:	E6AC898E67B4052375FDDFE9894B26D504A7827917BF3E02772CFF45C3FA7CC5E0EFFDC701D208E0DB89F05E42F195B1EC890F316BEE5CB8239AB45444DAA65 E
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 (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.673145545979894
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Shipping Documents Original BL, Invoice & Pa.exe
File size:	734208
MD5:	b89d3e7dd6ee20a09506365497f6cc3a
SHA1:	d5a40ae65560da802d5c5135d024d5fa8e840ff4
SHA256:	c2af0dcf4558a32fde15405648d8dd6410c51d319812755fcb8e4f742723bad7
SHA512:	9ffdf6633cc35a4cf2817ab9033d30d9377c83944e6b013aea5697a53c8d0772bf992305fcbbe18810bd4fa41aafcf7e31f517323f78eb0b637254a740281e09
SSDEEP:	12288:O2g1o0ezlROKMTSXHllp8maopsxu05K6zAyLe6NPBmFBdWM/QXPZ:bg1o9mOKSA9bzhLnNgXv/QB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..*.....I... ..`....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b49a6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6090F8E4 [Tue May 4 07:33:56 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb4954	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x404	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb29ac	0xb2a00	False	0.817510606193	data	7.68387820085	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x404	0x600	False	0.285807291667	data	2.3669114928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb6058	0x3a8	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Felix Jeyareuben 2012
Assembly Version	2.0.0.0
InternalName	ManifestEnvelope.exe
FileVersion	2.0
CompanyName	www.churchsw.org
LegalTrademarks	Church Software
Comments	
ProductName	Church Projector
ProductVersion	2.0
FileDescription	Church Projector
OriginalFilename	ManifestEnvelope.exe

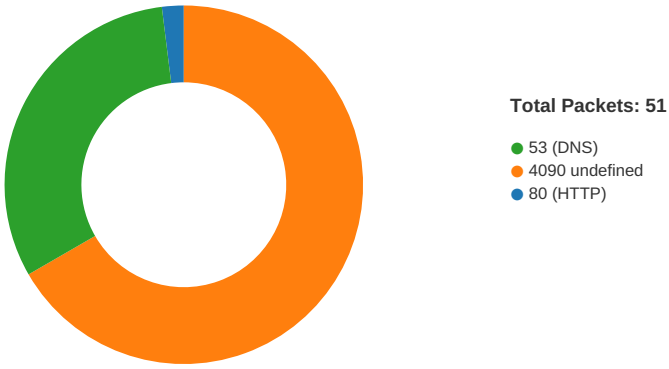
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-10:30:30.516363	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	4090	192.168.2.4	172.93.166.26
05/04/21-10:30:38.726516	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	4090	192.168.2.4	172.93.166.26

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-10:30:45.525830	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	4090	192.168.2.4	172.93.166.26
05/04/21-10:30:51.542446	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	4090	192.168.2.4	172.93.166.26
05/04/21-10:30:57.537521	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:02.522919	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:08.571572	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:15.430293	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:20.466887	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:26.477561	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:32.571814	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:37.631265	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:43.636714	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:49.661091	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	4090	192.168.2.4	172.93.166.26
05/04/21-10:31:56.624315	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	4090	192.168.2.4	172.93.166.26
05/04/21-10:32:03.661380	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	4090	192.168.2.4	172.93.166.26
05/04/21-10:32:09.718870	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	4090	192.168.2.4	172.93.166.26
05/04/21-10:32:15.719024	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	4090	192.168.2.4	172.93.166.26
05/04/21-10:32:20.736724	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	4090	192.168.2.4	172.93.166.26

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:30:25.946350098 CEST	49685	80	192.168.2.4	2.20.142.209
May 4, 2021 10:30:30.304523945 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:30.452847958 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:30.452972889 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:30.516362906 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:30.676390886 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:30.684725046 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:30.833106995 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:30.887154102 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:30.900424957 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.093060017 CEST	4090	49722	172.93.166.26	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:30:31.104357958 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104378939 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104394913 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104412079 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104429007 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104444981 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104463100 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104480028 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104491949 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.104513884 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104531050 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.104576111 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.104603052 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.254400015 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254445076 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254487038 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254544020 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254587889 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254587889 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.254622936 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.254627943 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254667044 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254688025 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.254705906 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254744053 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254762888 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.254791021 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254837036 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.254838943 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254889965 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254931927 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254967928 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.254968882 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.255007982 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.255016088 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.255089998 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.255127907 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.255141020 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.255175114 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.255217075 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.255227089 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.255265951 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.255323887 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405056000 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405106068 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405147076 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405184031 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405209064 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405220985 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405252934 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405260086 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405308008 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405308008 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405350924 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405400991 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405420065 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405457973 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405495882 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405509949 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405534029 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405570984 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405585051 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405610085 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405648947 CEST	4090	49722	172.93.166.26	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:30:31.405662060 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405695915 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405739069 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405744076 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405777931 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405816078 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405827045 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405854940 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405891895 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405911922 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.405930996 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405977964 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.405983925 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.406014919 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406070948 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406109095 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406120062 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.406153917 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.406166077 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406210899 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406249046 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406286955 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406296015 CEST	49722	4090	192.168.2.4	172.93.166.26
May 4, 2021 10:30:31.406323910 CEST	4090	49722	172.93.166.26	192.168.2.4
May 4, 2021 10:30:31.406342030 CEST	49722	4090	192.168.2.4	172.93.166.26

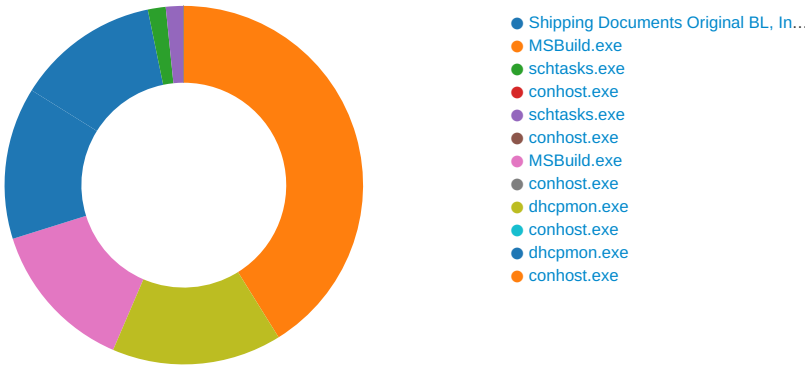
UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:30:08.362804890 CEST	61516	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:08.414283037 CEST	53	61516	8.8.8.8	192.168.2.4
May 4, 2021 10:30:09.153835058 CEST	49182	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:09.203901052 CEST	53	49182	8.8.8.8	192.168.2.4
May 4, 2021 10:30:09.926547050 CEST	59920	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:09.975424051 CEST	53	59920	8.8.8.8	192.168.2.4
May 4, 2021 10:30:10.701407909 CEST	57458	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:10.751379967 CEST	53	57458	8.8.8.8	192.168.2.4
May 4, 2021 10:30:11.596306086 CEST	50579	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:11.649147987 CEST	53	50579	8.8.8.8	192.168.2.4
May 4, 2021 10:30:12.713280916 CEST	51703	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:12.764913082 CEST	53	51703	8.8.8.8	192.168.2.4
May 4, 2021 10:30:13.953927040 CEST	65248	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:14.002691984 CEST	53	65248	8.8.8.8	192.168.2.4
May 4, 2021 10:30:14.819376945 CEST	53723	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:14.868194103 CEST	53	53723	8.8.8.8	192.168.2.4
May 4, 2021 10:30:15.610141993 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:15.658852100 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 10:30:16.914283991 CEST	65298	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:16.963977098 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 10:30:17.848736048 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:17.900161028 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 10:30:18.729810953 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:18.779098988 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 10:30:19.625092983 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:19.674388885 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 10:30:22.860003948 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:22.909003019 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 10:30:23.656889915 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:23.706955910 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 10:30:24.475920916 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 10:30:24.541471004 CEST	53	49257	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Shipping Documents Original BL, Invoice & Pa.exe PID: 5936
Parent PID: 6028

General

Start time:	10:30:14
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Shipping Documents Original BL, Invoice & Pa.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Shipping Documents Original BL, Invoice & Pa.exe'
Imagebase:	0xac0000
File size:	734208 bytes
MD5 hash:	B89D3E7DD6EE20A09506365497F6CC3A
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: 00000000.00000002.673275544.0000000003DD9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.673275544.0000000003DD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.673275544.0000000003DD9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.670633702.0000000002E4C000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D18CF06	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	6D18CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Shipping Documents Original BL, Invoice & Pa.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D49C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Shipping Documents Original BL, Invoice & Pa.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D49C907	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	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile

Analysis Process: MSBuild.exe PID: 5764 Parent PID: 5936

General

Start time:	10:30:24
Start date:	04/05/2021
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
Imagebase:	0xb10000
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	6D18CF06	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	6D18CF06	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	6BFDBEFF	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	6BFD1E60	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	6BFDBEFF	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	6BFDDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF57E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFD7038	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	6BFD1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF909.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFD7038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6BFDBEFF	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	6BFDBEFF	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	17	6BFD1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BFD1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BFD1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF57E.tmp	success or wait	1	6BFD6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpF909.tmp	success or wait	1	6BFD6A95	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	be 76 5e de d6 0e d9 48	.v^....H	success or wait	1	6BFD1B4F	WriteFile
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 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	6BFDDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF57E.tmp	unknown	1320	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6BFD1B4F	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\Framework\v4.0.30319\MSBuild.exe	success or wait	1	6BFD1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpF909.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	6BFD1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 60 2a 6b 5a 01 9a 4a 52 3c 82 e3 65 c4 38 82 91 01 e6 7a f6 be 12 4f ff 02 d1 9a f4 02 91 66 85 de 6d f3 50 51 3e 59 af e6 ea 7d a8 07 ef cb 08 4b ba 2c 4b 6c 2e 10 47 9c b5 f8 f5 fc 71 41 82 15 23 97 77 92 26 ba 81 37 6d c0 fb 42 a8 49 ce b2 da 9d 0f 00 cb 69 6e b1 83 3c 35 4a b9 12 95 81 7a 29 cb 48 3f e1 cd c0 f1 a9 36 ad e0 2a 32	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... `*kZ..JR<..e.8....z...O..... f..m.PQ>Y...}.....K.,Kl..G.... .qA..#.w.&..7m..B.I.....in.. <5J....z).H?.....6..*2	success or wait	8	6BFD1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	315512	8f ae 66 23 20 c2 13 cc d4 29 31 5c 2a 95 0a a5 1e a8 35 f4 e1 c6 b2 e5 3b f0 54 f4 d8 75 8d e7 ab 20 ff 33 b7 58 64 0c e9 1f 20 80 b6 85 02 75 28 ff 8e b5 5f c1 56 f7 7b 4c a2 0a 59 d2 b4 38 cb 95 a5 ce 0d 7e 85 f6 f8 53 37 39 d8 a9 66 30 56 b3 9a e2 3d e3 7d 0d a4 a0 53 4a 67 7c b6 6c 68 06 4a 1a db 5e 47 65 a8 0b fc 8e 17 f2 fe bc 1c 33 68 3f 6e 8e 9f 3a d1 bf e1 72 a8 fa 9f d2 2c 6f c7 22 61 c6 49 d2 01 83 02 5c c3 8e e8 30 5a e8 44 9a bd b8 1e fb fa c5 f4 f1 dc 82 5e b3 06 0c c3 5b 2e ea 66 ce 49 bc bd eb ce 40 2f 5f e7 cc 22 f1 8b 35 2b 02 0a ff 49 0b a7 de 4a 60 f4 2f 73 af 8d 70 2d a3 1a b9 bf f5 63 0e 87 3f e7 1f f6 2a 06 c7 20 0e 26 99 8b c3 8f f5 b0 3e b2 59 65 24 3d 0b 70 47 05 e3 19 93 df bf 39 44 dd c1 d1 27 37 1a 77 d2 61 d9 5b 33 e5 a1 a9	..f# ....)1*.....5.....;.T..u... .3.Xd... ....u(..._.V.{L.. Y..8.....~...S79..f0V...=.}... SJg|.lh.J..^Ge.....3h?n..: ...r....,o."a.I....\...0Z.D... ....^....[..f.I....@/_..". .5+...I...J`./s..p-.....c..?...*.. .&......>.Ye$=.pG.....9D ...'7.w.a.[3...	success or wait	1	6BFD1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	6BFD1B4F	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	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D165705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D16CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D14D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D14D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	4096	success or wait	1	6D14D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	512	success or wait	1	6D14D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D165705	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6BFD646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 5792 Parent PID: 5764

General

Start time:	10:30:26
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpF57E.tmp'
Imagebase:	0x1310000
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\tmpF57E.tmp	unknown	2	success or wait	1	131AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF57E.tmp	unknown	1321	success or wait	1	131ABD9	ReadFile

Analysis Process: conhost.exe PID: 5788 Parent PID: 5792

General

Start time:	10:30:27
Start date:	04/05/2021
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: 1680 Parent PID: 5764

General

Start time:	10:30:27
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpF909.tmp'
Imagebase:	0x1310000
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\tmpF909.tmp	unknown	2	success or wait	1	131AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF909.tmp	unknown	1311	success or wait	1	131ABD9	ReadFile

Analysis Process: conhost.exe PID: 1492 Parent PID: 1680

General

Start time:	10:30:28
Start date:	04/05/2021
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: 1556 Parent PID: 968

General

Start time:	10:30:28
Start date:	04/05/2021
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:	0x1e0000
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	6D49C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6BFD1B4F	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	6BFD1B4F	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	6BFD1B4F	WriteFile
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	6D49C907	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	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6D16CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.rsp	unknown	4096	success or wait	1	6BFD1B4F	ReadFile

Analysis Process: conhost.exe PID: 1364 Parent PID: 1556

General

Start time:	10:30:28
Start date:	04/05/2021

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: 980 Parent PID: 968

General

Start time:	10:30:31
Start date:	04/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x5c0000
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	6D18CF06	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	6D18CF06	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	6D49C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6BFD1B4F	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 4.0.3031 9.42000]..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6BFD1B4F	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	6BFD1B4F	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	6D49C907	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	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile

Analysis Process: conhost.exe PID: 4116 Parent PID: 980

General

Start time:	10:30:32
Start date:	04/05/2021
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: 5728 Parent PID: 3424

General

Start time:	10:30:39
Start date:	04/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xf80000
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	6D18CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D18CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6BFD1B4F	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	6BFD1B4F	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	6BFD1B4F	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	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFD1B4F	ReadFile

Analysis Process: conhost.exe PID: 4804 Parent PID: 5728

General

Start time:	10:30:39
Start date:	04/05/2021
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

Disassembly

Code Analysis