ID: 337536
Sample Name: shipping order#.scr
Cookbook: default.jbs
Time: 18:27:13
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

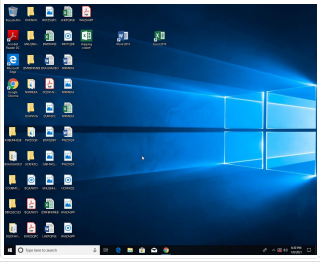
Analysis Report shipping order#.scr

Overview

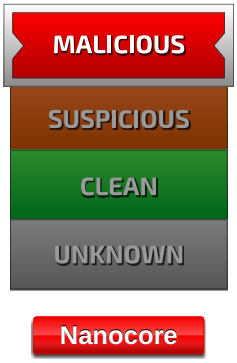
General Information

Sample Name:	shipping order#.scr (renamed file extension from scr to exe)
Analysis ID:	337536
MD5:	a916070df947a28.
SHA1:	2c4215352fecfbd..
SHA256:	b657538bf8bc1ac..
Tags:	DEU Endurance geo Nan oCore nVpn RAT scr

Most interesting Screenshot:



Detection



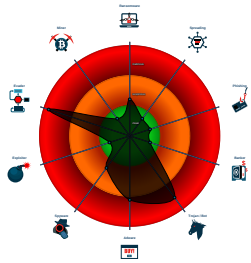
Nanocore

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Powershell adding …
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- Connects to a pastebin service (like…
- Contains functionality to hide a threa…
- Creates an undocumented autostart …
- Creates autostart registry keys with …
- Creates multiple autostart registry ke…

Classification



Startup

- **System is w10x64**
- shipping order#.exe (PID: 5884 cmdline: 'C:\Users\user\Desktop\shipping order#.exe' MD5: A916070DF947A28EA73074C080189D35)
  - powershell.exe (PID: 5796 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5128 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4944 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6836 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\shipping order#.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6996 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6948 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 2460 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5136 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 4176 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7124 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - shipping order#.exe (PID: 6648 cmdline: C:\Users\user\Desktop\shipping order#.exe MD5: A916070DF947A28EA73074C080189D35)
  - WerFault.exe (PID: 5824 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5884 -s 2396 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- shipping order#.exe (PID: 5812 cmdline: 'C:\Users\user\Desktop\shipping order#.exe' MD5: A916070DF947A28EA73074C080189D35)
  - powershell.exe (PID: 1836 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2848 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6880 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- shipping order#.exe (PID: 6440 cmdline: 'C:\Users\user\Desktop\shipping order#.exe' MD5: A916070DF947A28EA73074C080189D35)
- shipping order#.exe (PID: 6476 cmdline: 'C:\Users\user\Desktop\shipping order#.exe' MD5: A916070DF947A28EA73074C080189D35)
- shipping order#.exe (PID: 408 cmdline: 'C:\Users\user\Desktop\shipping order#.exe' MD5: A916070DF947A28EA73074C080189D35)
- shipping order#.exe (PID: 5700 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' MD5: A916070DF947A28EA73074C080189D35)
- dhcpmon.exe (PID: 5392 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: A916070DF947A28EA73074C080189D35)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.953347947.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000016.00000002.953347947.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000016.00000002.953347947.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Process Memory Space: shipping order#.exe PID: 6648	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x151827:$x1: NanoCore.ClientPluginHost • 0x151888:$x2: IClientNetworkHost • 0x156c8d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x164bff:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Process Memory Space: shipping order#.exe PID: 6648	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.shipping order#.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
22.2.shipping order#.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
22.2.shipping order#.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
22.2.shipping order#.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

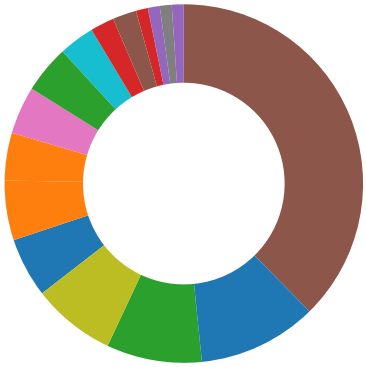
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Powershell adding suspicious path to exclusion list

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Connects to a pastebin service (likely for C&C)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Creates an undocumented autostart registry key

Creates autostart registry keys with suspicious names

Creates multiple autostart registry keys

Drops PE files to the startup folder

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

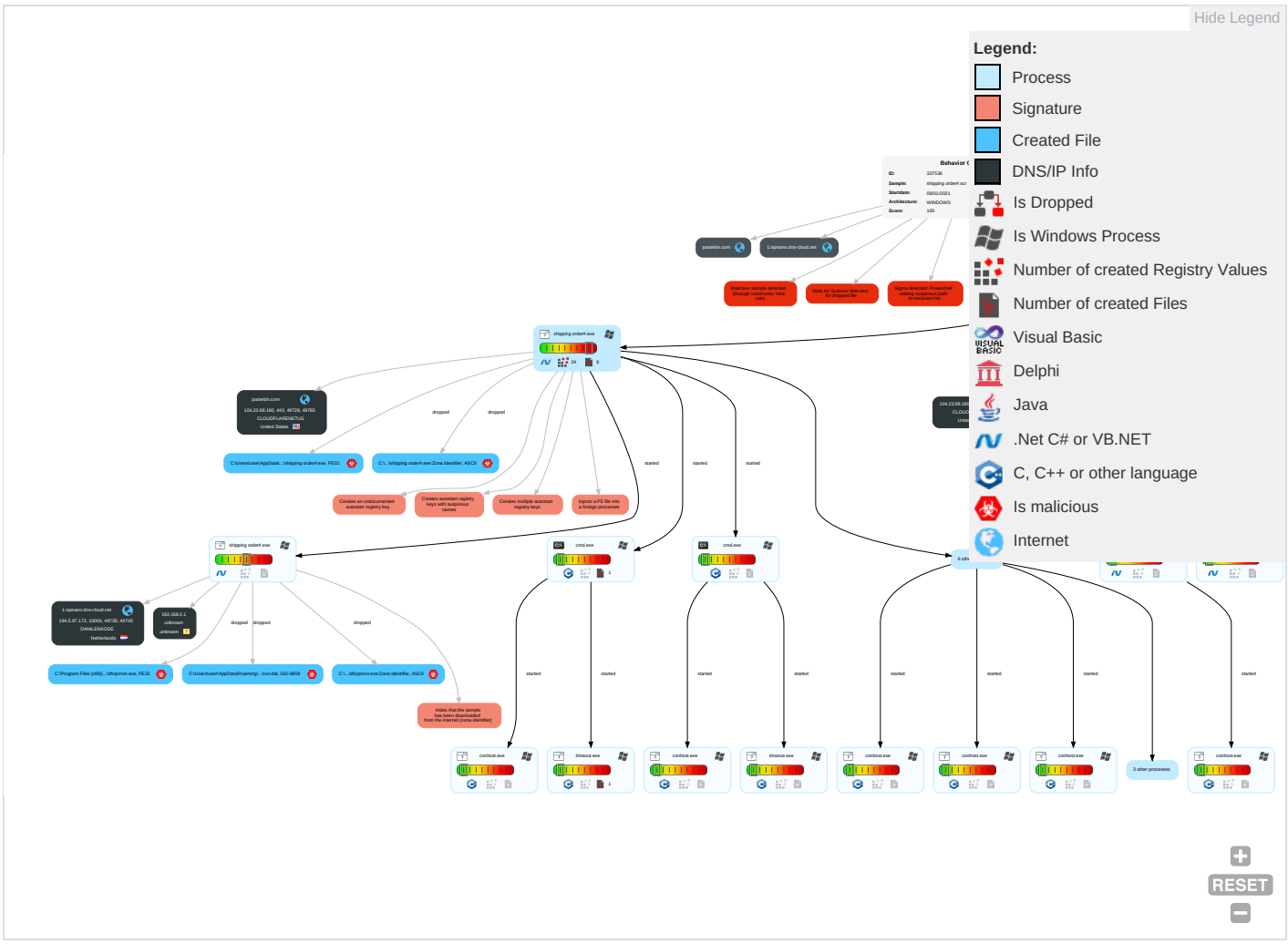
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Valid Accounts	Windows Management Instrumentation 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1 1	Input Capture 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1	
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 4 2 1	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 2 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 4 2 1	Obfuscated Files or Information 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Security Software Discovery 5 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 2 5	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 5	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	

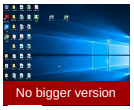
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
shipping order#.exe	30%	ReversingLabs	Win32.Trojan.Wacatac	
shipping order#.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order #.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	30%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order #.exe	30%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.2.shipping order#.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File

Domains

Source	Detection	Scanner	Label	Link
1.ispnano.dns-cloud.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://logo.vGs	0%	Avira URL Cloud	safe	
http://https://go.microd	0%	Avira URL Cloud	safe	
http://crl.globalsi7	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

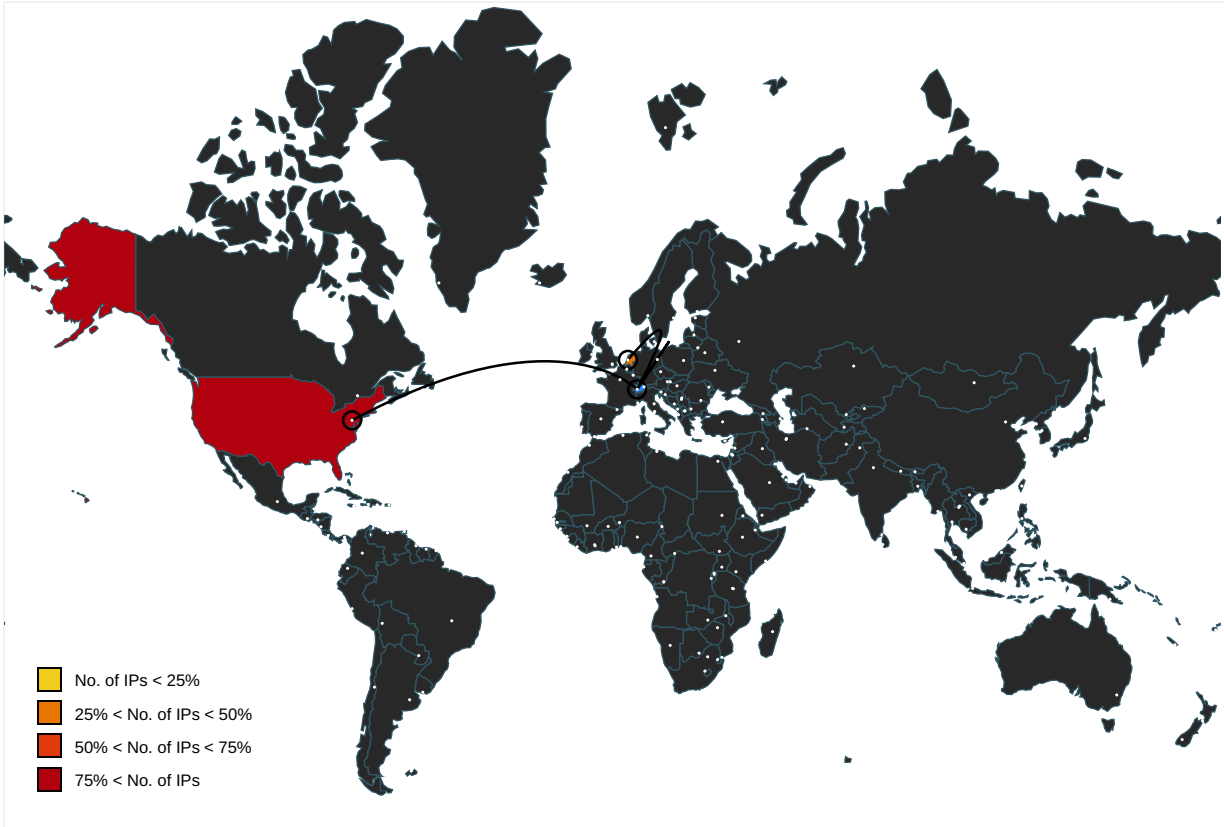
Name	IP	Active	Malicious	Antivirus Detection	Reputation
1.ispnano.dns-cloud.net	194.5.97.173	true	false	• 1%, Virustotal, Browse	unknown
pastebin.com	104.23.98.190	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000003.00000003.881997379.0000000004F9E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://https://pastebin.com/raw/W63zsRav	shipping order#.exe, 00000015.00000003.1039301625.00000000032B4000.00000004.00000001.sdmp	false		high
http://logo.vGs	powershell.exe, 00000025.00000003.844054876.0000000007D63000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://https://go.microd	powershell.exe, 00000004.00000003.945556965.0000000005233000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprinthttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	shipping order#.exe, 00000000.00000003.657555811.00000000033E8000.00000004.00000001.sdmp, shipping order#.exe, 0000000F.00000003.813659881.00000000029D4000.00000004.00000001.sdmp, shipping order#.exe, 00000015.00000003.910702496.0000000002CE5000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddresszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://crl.globalsi7	powershell.exe, 00000025.00000003.844054876.0000000007D63000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000001B.00000003.809038386.00000000059D0000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.23.99.190	unknown	United States		13335	CLOUDFLARENETUS	false
194.5.97.173	unknown	Netherlands		208476	DANILENKODE	false
104.23.98.190	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337536
Start date:	08.01.2021
Start time:	18:27:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shipping order#.scr (renamed file extension from scr to 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:	40
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.adwa.evad.winEXE@58/24@27/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.193.48, 51.11.168.160, 168.61.161.212, 52.255.188.83, 93.184.221.240, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.144.132, 40.126.1.130, 40.126.1.166, 20.190.129.24, 20.190.129.130, 40.126.1.128, 20.190.129.2, 40.126.1.145, 20.190.129.19, 104.43.139.144 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, www.tm.a.prd.aadg.akadns.net, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing behavior and disassembly information. • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:28:06	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\shipping order#.exe
18:28:15	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run shipping order#.exe C:\Users\user\Desktop\shipping order#.exe
18:28:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\shipping order#.exe
18:28:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run shipping order#.exe C:\Users\user\Desktop\shipping order#.exe
18:28:40	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe
18:28:41	API Interceptor	753x Sleep call for process: shipping order#.exe modified
18:28:54	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:29:12	API Interceptor	159x Sleep call for process: powershell.exe modified

Time	Type	Description
18:30:33	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run dhcpmon.exe C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:30:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run dhcpmon.exe C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:30:55	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.23.99.190	7fYoHeaCBG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	r0QRptqiCl.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	JDgYMW0LHW.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	kigAlmMyB1.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	5T4Ykc0VSK.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	afvhKak0Ir.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	1KITgJnGbl.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	DovV3LuJ6l.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	66f8F6WvC1.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PxwWcmbMC5.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	XnAJZR4NcN.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	uqXsQvWMnL.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	l8r7e1pqac.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VrR9J0FnSG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	dEpoPWHmoI.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	zZp3oXclum.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	aTZQZVVriQ.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	U23peRXm5Z.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	eXP2pYucWu.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	L6UBlWyCpV.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pastebin.com	0IO1Or2045.exe	Get hash	malicious	Browse	• 104.23.98.190
	OVl2ydWZDb	Get hash	malicious	Browse	• 104.23.98.190
	PO20002106.exe	Get hash	malicious	Browse	• 104.23.99.190
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.98.190
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.99.190
	Ema.exe	Get hash	malicious	Browse	• 104.23.98.190
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 104.23.99.190
	TOP URGENT RFQ 2021 Anson Yang.exe	Get hash	malicious	Browse	• 104.23.98.190
	sample details.exe	Get hash	malicious	Browse	• 104.23.99.190
	zrr4Nw19.exe	Get hash	malicious	Browse	• 104.23.99.190
	TF5wEGc1Fp.exe	Get hash	malicious	Browse	• 104.23.99.190
	image002933894HF8474H038RHF7.exe	Get hash	malicious	Browse	• 104.23.98.190
	IMG-PO-SCAN-DOCUMENTS-00HDU12.exe	Get hash	malicious	Browse	• 104.23.98.190
	ZdCDLe85.exe	Get hash	malicious	Browse	• 104.23.99.190
	IMAGE-SCAN-DOCUMENTS-002D.exe	Get hash	malicious	Browse	• 104.23.98.190
	NEW ORDER.pdf.exe	Get hash	malicious	Browse	• 104.23.99.190
	KnXebI2hpX.exe	Get hash	malicious	Browse	• 104.23.99.190
	httpscdndiscordappcomattachments785319022966997035 791667564027052052aGBWK3jv8vMhTU3.exe	Get hash	malicious	Browse	• 104.23.99.190
	sz.exe	Get hash	malicious	Browse	• 104.23.99.190
	Confirmation Copy RefNo-MT102.exe	Get hash	malicious	Browse	• 104.23.99.190

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	BL,IN&PL.exe	Get hash	malicious	Browse	• 194.5.97.206
	New PO.exe	Get hash	malicious	Browse	• 194.5.98.32
	Order Inquiry.exe	Get hash	malicious	Browse	• 194.5.97.235
	IMG 01-06-2021 93899283.exe	Get hash	malicious	Browse	• 194.5.97.177
	SWIFT345343445pdf.exe	Get hash	malicious	Browse	• 194.5.97.164
	DHL1.exe	Get hash	malicious	Browse	• 194.5.98.145
	Original BL_pdf.exe	Get hash	malicious	Browse	• 194.5.97.107
	AWB & CI_pdf.exe	Get hash	malicious	Browse	• 194.5.97.107
	File.exe	Get hash	malicious	Browse	• 194.5.98.108
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 194.5.98.215
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	Shiping Doc BL.exe	Get hash	malicious	Browse	• 194.5.98.157
	INV_2021354783263530001.exe	Get hash	malicious	Browse	• 194.5.98.211
	SWB copy.exe	Get hash	malicious	Browse	• 194.5.98.108
	DHL FI.exe	Get hash	malicious	Browse	• 194.5.98.145
	DHL DETAILS.exe	Get hash	malicious	Browse	• 194.5.98.145
CLOUDFLARENETUS	0939489392303224233.exe	Get hash	malicious	Browse	• 162.159.128.233
	KeyMaker.exe	Get hash	malicious	Browse	• 1.0.0.0
	b12d7feb3507461a.exe	Get hash	malicious	Browse	• 162.159.138.232
	ARCH_2021.doc	Get hash	malicious	Browse	• 172.67.141.14
	SecuriteInfo.com.Trojan.DownLoader36.32796.17922.exe	Get hash	malicious	Browse	• 162.159.137.232
	0IO1Or2045.exe	Get hash	malicious	Browse	• 104.23.98.190
	y46XVvLaVc.exe	Get hash	malicious	Browse	• 172.67.166.210
	FTH2004-005.exe	Get hash	malicious	Browse	• 23.227.38.74
	inv.exe	Get hash	malicious	Browse	• 104.27.152.121
	promotion.exe	Get hash	malicious	Browse	• 104.27.201.87
	ul9kpUwYel.xls	Get hash	malicious	Browse	• 104.22.1.232
	F6D24k8j9o.exe	Get hash	malicious	Browse	• 104.28.5.151
	36.exe	Get hash	malicious	Browse	• 104.28.8.109
	IKWSLxGlrQ.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• 104.16.18.94
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 104.16.18.94
	http://https://www.food4rhino.com/app/human	Get hash	malicious	Browse	• 104.16.18.94
	OKU-010920 SCQ-220920.doc	Get hash	malicious	Browse	• 104.24.113.40
	http://https://www.food4rhino.com/app/elefront	Get hash	malicious	Browse	• 104.16.18.94
	INFO.doc	Get hash	malicious	Browse	• 104.18.61.59
CLOUDFLARENETUS	0939489392303224233.exe	Get hash	malicious	Browse	• 162.159.128.233
	KeyMaker.exe	Get hash	malicious	Browse	• 1.0.0.0
	b12d7feb3507461a.exe	Get hash	malicious	Browse	• 162.159.138.232
	ARCH_2021.doc	Get hash	malicious	Browse	• 172.67.141.14
	SecuriteInfo.com.Trojan.DownLoader36.32796.17922.exe	Get hash	malicious	Browse	• 162.159.137.232
	0IO1Or2045.exe	Get hash	malicious	Browse	• 104.23.98.190
	y46XVvLaVc.exe	Get hash	malicious	Browse	• 172.67.166.210
	FTH2004-005.exe	Get hash	malicious	Browse	• 23.227.38.74
	inv.exe	Get hash	malicious	Browse	• 104.27.152.121
	promotion.exe	Get hash	malicious	Browse	• 104.27.201.87
	ul9kpUwYel.xls	Get hash	malicious	Browse	• 104.22.1.232
	F6D24k8j9o.exe	Get hash	malicious	Browse	• 104.28.5.151
	36.exe	Get hash	malicious	Browse	• 104.28.8.109
	IKWSLxGlrQ.exe	Get hash	malicious	Browse	• 172.67.188.154
	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• 104.16.18.94
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 104.16.18.94
	http://https://www.food4rhino.com/app/human	Get hash	malicious	Browse	• 104.16.18.94
	OKU-010920 SCQ-220920.doc	Get hash	malicious	Browse	• 104.24.113.40
	http://https://www.food4rhino.com/app/elefront	Get hash	malicious	Browse	• 104.16.18.94
	INFO.doc	Get hash	malicious	Browse	• 104.18.61.59

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	F6D24k8j9o.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	umOXxQ9PFS.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	IKWSLxGlrQ.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Softerra Adaxes 2011.3.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	DSj7ak0N6l.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	3AD78RVleO.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	rFUaUAKfPi.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	QWP-0716.xls.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	invoice-ID3626307348012.vbs	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	xPcTV1mh3w.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	SecuriteInfo.com.Trojan.GenericKD.36004001.8844.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Manager[1].exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	PO20002106.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Payment Documents.xls	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	QPI-01458.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	LITmNphcCA.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	HSBC Payment Advice - HSBC67628473234[20201412].exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Ema.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Setup_6953.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\shipping order#.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2818048
Entropy (8bit):	3.8180432062188556
Encrypted:	false
SSDEEP:	24576:D+zmQLwh3i3PO/o1U6kUnu6l+4RcblO7O0uX7JgINl9jnxjdNBGqwe:KY3i3POEFWZ0kJfh4e
MD5:	A916070DF947A28EA73074C080189D35
SHA1:	2C4215352FECFBD74B596F1125177F54CD010A4B
SHA-256:	B657538BF8BC1ACA7CA8E7E02F1C5A39CBC8BC343BF7C5EBFE026F6DCC02FE32
SHA-512:	3D5B554C97D6A093F6CE94B8C5D681438F5F4B74DF391468E8ADF36A7AB2B599B0EE49DCF7C57FB9AAB03509D3F6A07747D94E05929EAAF627AA18D170ABFCE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*._.....p(.....(.. ....(...@.. .....`+.....(. ..@.....<.(.O.....(.....t(.....@+..... ..... ..H.....text....o(.. ...p(..... ..`.rsrc.....(.....r(.....@..@.reloc .....@+.....*.....@..B.....p.(.....H.....'.....|.....*.r...p.....r...p.....r...p.....s.....s}.....*6.~....o....&**....(....*~~.....:....(....s(.....~....*. ....*2r..!p.(....*2r.!p.(....*2r..!p.(....*2r&.!p.(....*2rD.!p.(....*2rx.!p.(....*2r..!p.(....*2r.!p.(....*..%...(....*~~.....:....([...s(.....~....*.....90...(....9.....r .!p....(-...(%...*.....(....*....*2r..!p. (....*2r.!p.(....*2r.!p.(....*2r..!p.(....*2r..!p.(....*2r2.!p.(....*2

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

Process:	C:\Users\user\Desktop\shipping order#.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DEE.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8446
Entropy (8bit):	3.6972961175464687
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiHS6r6YreSUMdQDgmfZMSR+prE89b0gsf0cYcm:RrlsNiy6r6YiSUMdQDgmfeSU0zf/C
MD5:	A0BEA0FAF8565FF7214B619B29C01B18
SHA1:	DA8B2DA5D9EF299A4BDED31783623B710E19B76E
SHA-256:	AD60AF38E7250AF54CF9B71921C1027BC7E2676EB232EB31513E88541E071D80
SHA-512:	86D6B867CAE0D7BE5045AF04369954D53944AA2DD7CEE5446D72622782175A8379B80FEF6C06FDFEB27CB9400AE11E67A81AAE704F12790171459BA2DD508A0
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DEE.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.8.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3D9.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4733
Entropy (8bit):	4.471986333355066
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9YWWSC8BE8fm8M4J7o5VFFiP+q8vV5VWtigGwtUBU5d:uITfAb3SN/JC8PK3M8K5d
MD5:	82A0B5CCAF7F4CD4E6DCC88F578897BB
SHA1:	34D4E7FF71C1E3F075211F17A21BE8C5DAB7DF81
SHA-256:	4A1B007851B2E84B9422959F8741016F5C34A04BD3FF4366500B2B21BD5DEFEE
SHA-512:	2C11A592CC8B7C616D12137A7D1D09A7EFA0819F2F1822AC25F10ACF4A36BCD98DE0DD6C0F6726010CD65D4A98A82F1E37A25CEA9EA79E5F9AEBD0C1175E6B8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="808000" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jan 8 17:29:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	333257
Entropy (8bit):	3.7424784924409673
Encrypted:	false
SSDEEP:	3072:bz+UvrX0gpjd+p31HIaOZYee8Hq9gIOgF5Wo/0WtUCgUaSvpb1qDXFJj:bK0X0geppqK9RpDWu1tTjDOJj
MD5:	84FB07A24E4790983A5FB88400CF1A93
SHA1:	3DD6827693BAB8D6576E602BBBC039652A3DDA66
SHA-256:	615101E8378ED1B6BCED34E4D2503838EA67410651E85663ABF1D6DB8FB1C18F
SHA-512:	77E72261DABA22EBB5CF4C84B2AAC3BAEBDEDA8F193E553C201CE901F64F04E5C27E07D77B479D84FB208E8B84A4873A4392A2AD23E92C1A1B841CFC00B666E5
Malicious:	false
Preview:	MDMP..... .....r..._.....U.....B.....1.....GenuineIntelW.....T....._.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	698
Entropy (8bit):	5.068223855918045
Encrypted:	false
SSDEEP:	12:reMPyMYx2Y5BYtmWNUc5AtYX5E4a2KyrNpyMYGH+ptsxptsOtw9O9S8:reKyMGF5ytmLcetYX5E2KyPyMb+zsxzN
MD5:	684C50BD02AF31C87EA2FE17C2AF71CE
SHA1:	930B39970E6AF00CD0C1E203478D25848D4CEB4C
SHA-256:	A68A09639C8190A5710DF0DF0693BBADB11F453197BF44339382B813CA048EA2
SHA-512:	B919F1A138A2F1BD67734FA5CBC0EED6C54D12C25835097E2F1753F44A300E6F2BE0250A85BCC5FD606E329BDA42DB2329BF7826E93EAED47C68CD6213D9CF3
Malicious:	false
Preview:	PSMODULECACHE.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D.....C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation.....Invoke-OperationValidation.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_brge2zcm.hwd.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_czsau0n1.mqj.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_e04p2qly.o2t.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fraa5aiu.gcp.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_harhvbow.ned.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pilnwesf.xu0.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_x2khrpam.ug2.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yf4s2bry.3jw.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\shipping order#.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:4zu:r
MD5:	13AFD6B42F94B15B991447EC048184D4
SHA1:	EC207DE4EE368BE199302725DE3A7B1D1948AAAB
SHA-256:	62E4FE80D7F5FD8715432E7CF2432CFF6E4550B043D78016E4054F8AA40B3BB1
SHA-512:	54C232BB4B6C525254767760E3FE355518565D5CB428F6C849F64AD0A4757722A7AA36E6D612FAADCE1C9AF7BB69CA83C99C8634B41091176C3181208E7F92BA
Malicious:	**true**
Preview:	.....H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe	
Process:	C:\Users\user\Desktop\shipping order#.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2818048
Entropy (8bit):	3.8180432062188556
Encrypted:	false
SSDEEP:	24576:D+zmQLwh3i3PO/o1U6kUnu6l+4RcblO7O0uX7JgINl9jnxjdNBGqwe:KY3i3POEFWZ0kJfh4e
MD5:	A916070DF947A28EA73074C080189D35
SHA1:	2C4215352FECFBD74B596F1125177F54CD010A4B
SHA-256:	B657538BF8BC1ACA7CA8E7E02F1C5A39CBC8BC343BF7C5EBFE026F6DCC02FE32
SHA-512:	3D5B554C97D6A093F6CE94B8C5D681438F5F4B74DF391468E8ADF36A7AB2B599B0EE49DCF7C57FB9AAB03509D3F6A07747D94E05929EAAF627AA18D170ABFC E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*._.....p(.....(.. ....(...@.. .....`+.....(. ..@.....<.(.O.....(.....t(.....@+..... ..... ..H.....text....o(.. ...p(..... ..`.rsrc.....(.....r(.....@..@.reloc .....@+.....*.....@..B.....p.(.....H.....'....|.....*.r...p.....r...p.....r...p.....s.....s}.....*6.~....o....&**....(....*~~.....:....(....s(.....~....*. ....*2r..!p.(....*2r.!p.(....*2r..!p.(....*2r&.!p.(....*2rD.!p.(....*2rx.!p.(....*2r..!p.(....*2r.!p.(....*..%...(....*~~.....:....([...s(.....~....*.....90...(....9.....r .!p....(-...(%...*.....(....*....*2r..!p. (....*2r.!p.(....*2r.!p.(....*2r..!p.(....*2r..!p.(....*2r2.!p.(....*2

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\shipping order#.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210108\PowerShell_transcript.701188.Laubqkk7.20210108182807.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	962
Entropy (8bit):	5.31514815011842
Encrypted:	false
SSDEEP:	24:BxSAJ7vBZRJNzx2DOXUWeSuamuVM52WMHjeTKKjX4CIym1ZJXLduamuVM5a:BZFvjTZoO+SGuaxMqDYB1ZhdGuaa
MD5:	85C3FC216E604D6B70C5FC72D0822EBA
SHA1:	66D0F3A14FD0AAB7DA5490E8DF26EC857513B590
SHA-256:	BF4747B169A4C9628AD16514F6226751AF0B95835642039BE075425E4492208D
SHA-512:	D49605C11AB2565DBBB0D0872D5C6AB3D454BF3C69C8F7B9D0C0977FB37BF81EE5E4AA1BF8F43C787649487CAF3979C7EA8D1EA57B9CDDED452FDDB4C0B8 D45

C:\Users\user\Documents\20210108\PowerShell_transcript.701188.Laubqkk7.20210108182807.txt	
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108182839..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe -Force..Process ID: 5128..PSVersion: 5.1.17134.1. .PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0 ..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210108182839..********** *..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe -Force..

C:\Users\user\Documents\20210108\PowerShell_transcript.701188.ONgqdUkt.20210108182809.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	854
Entropy (8bit):	5.295052882573072
Encrypted:	false
SSDEEP:	24:BxSAp7vBZRJNzx2DOXUWeSuaq2WZ3HjeTKKjX4CIym1ZJXJFuaqa:BZlvjTZoO+SKxZ3qDYB1ZbFKa
MD5:	D3D23BDEB4FAF32D392FF68964B083A2
SHA1:	BE69E101BFB81A2BC3E236257B0FB70F5A9074EC
SHA-256:	8D793883D177D66F26A6104CD1C4F4C11A9CE0D52A973A6C52798D5ACFD2A204
SHA-512:	12952AC76FC6B49C9F63C337A72A1BFC2DE9904CF7D1A1F32EC87579F8400C4A1C9989F5C809EB973A5B3B608F430DDFD84296C594D1919169A2D516DAC714E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108182848..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\shipping order#.exe -Force..Process ID: 6836..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210108182851..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\shipping order#.exe -Force..

C:\Users\user\Documents\20210108\PowerShell_transcript.701188.nGv+RGBh.20210108182808.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	962
Entropy (8bit):	5.313331889731213
Encrypted:	false
SSDEEP:	24:BxSAs7vBZRJNzx2DOXUWeSuamuVM52WNHjeTKKjX4CIym1ZJX2uamuVM5a:BZqvjTZoO+SGuaxNqDYB1ZsGuaa
MD5:	3DE15C085E769AA01B1A201BAE5C465F
SHA1:	B236DB49D392ACC323ABA55E5EDCD72B77281519
SHA-256:	3BE51DEAACE729D430113C7F776200060DEAE5B640EF686D6FF950311E3676AA
SHA-512:	F0D862703E139FFF831530AF5E4FD637C3CF351AFC1055A9817CE41C30E908E9E049DBE7E76C79C567266AB1EEB998EFFF8E769CDBE8C9AB30C174ABBB37F40
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108182847..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe -Force..Process ID: 4944..PSVersion: 5.1.17134.1. .PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0 ..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210108182847..********** *..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe -Force..

C:\Users\user\Documents\20210108\PowerShell_transcript.701188.tt6CRrQ7.20210108182806.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	962
Entropy (8bit):	5.319360174397925
Encrypted:	false
SSDEEP:	24:BxSAM7vBZRJNzx2DOXUWeSuamuVM52W9HjeTKKjX4CIym1ZJXWuamuVM5a:BZKvjTZoO+SGuax9qDYB1ZQGuaa
MD5:	BC0A8E8EED11BE498F474112A53D9537
SHA1:	A101FA3A0C1D2DEC525760A7F44BE5FC97AE1DBE
SHA-256:	1B8269998180214C2D74A8D6F432D63C7646B1D3046CCC96496FA186DF473838
SHA-512:	52FDB1297269B0113477030F9A4DCD710D495199A4141B56968BB9D8EF8DA663ACD67F4370D8E5759344D9B09A60C9A3BA5F15F84D510A089B3CE0EF0EC05A0
Malicious:	false

C:\Users\user\Documents\20210108\PowerShell_transcript.701188.tt6CRrQ7.20210108182806.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108182836..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe -Force..Process ID: 5796..PSVersion: 5.1.17134.1. .PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0 ..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210108182836..********** *..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe -Force..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	3.8180432062188556
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	shipping order#.exe
File size:	2818048
MD5:	a916070df947a28ea73074c080189d35
SHA1:	2c4215352fecfbd74b596f1125177f54cd010a4b
SHA256:	b657538bf8bc1aca7ca8e7e02f1c5a39cbc8bc343bf7c5ebfe026f6dcc02fe32
SHA512:	3d5b554c97d6a093f6ce94b8c5d681438f5f4b74df391468e8adf36a7ab2b599b0ee49dcf7c57fb9aab03509d3f6a07747d94e05929eaaf627aa18d170abfc4e
SSDEEP:	24576:D+zmQLwh3i3PO/o1U6kUnu6l+4RcblO7O0uX7JgINl9jnxjdNBGqwe:KY3i3POEFWZ0kJfh4e
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.... *._.....p(.....(.. ....(...@.. .....`+.....(...@.....

File Icon

Icon Hash:	07d8d8d4d4d85026

Static PE Info

General

Entrypoint:	0x688f8e
Entrypoint Section:	.text
Digitally signed:	true
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:	0x5FF82A12 [Fri Jan 8 09:46:58 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

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x288f3c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x28a000	0x28adc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x287400	0x15a0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2b4000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x286f94	0x287000	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x28a000	0x28adc	0x28c00	False	0.0469049559049	Macintosh MFS data (locked) created: Mon Apr 24 18:35:32 2017, last backup: Mon May 29 23:14:11 1995, block size: 2110829513, number of blocks: 17063, volume name: \246\330	2.9711901807	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2b4000	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_ICON	0x28a268	0xc35	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x28aea0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4280119364, next used block 4280119364		
RT_ICON	0x29b6c8	0x94a8	data		
RT_ICON	0x2a4b70	0x5488	data		
RT_ICON	0x2a9ff8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x2ae220	0x25a8	data		
RT_ICON	0x2b07c8	0x10a8	data		
RT_ICON	0x2b1870	0x988	data		
RT_ICON	0x2b21f8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x2b2660	0x84	data		
RT_VERSION	0x2b26e4	0x3f8	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

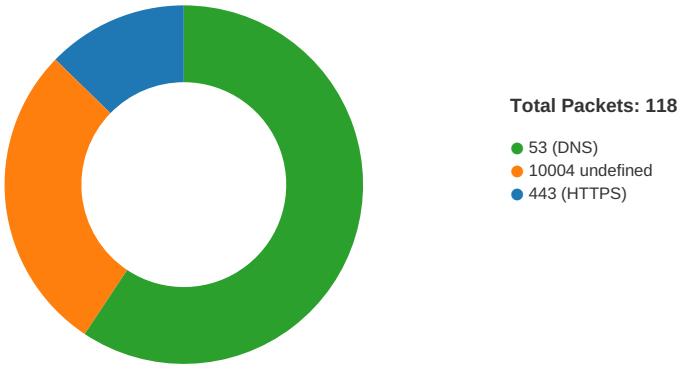
Description	Data
LegalCopyright	Microsoft Corp. All rights reserved.
FileVersion	2011.110.2809.27
CompanyName	Microsoft Corporation
LegalTrademarks	Microsoft SQL Server is a registered trademark of Microsoft Corporation.
Comments	SQL
ProductName	Microsoft SQL Server
ProductVersion	11.0.2809.27
FileDescription	SQL External minidumper
Guid	4c600aad-49bf-420d-b1b2-61d4bf3fb135
Translation	0x0000 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:28:09.279190063 CET	49728	443	192.168.2.4	104.23.98.190
Jan 8, 2021 18:28:09.320250034 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.321468115 CET	49728	443	192.168.2.4	104.23.98.190
Jan 8, 2021 18:28:09.362423897 CET	49728	443	192.168.2.4	104.23.98.190
Jan 8, 2021 18:28:09.403578997 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.406205893 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.406260967 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.406292915 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.407135963 CET	49728	443	192.168.2.4	104.23.98.190
Jan 8, 2021 18:28:09.412537098 CET	49728	443	192.168.2.4	104.23.98.190
Jan 8, 2021 18:28:09.455337048 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.456012964 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.499023914 CET	49728	443	192.168.2.4	104.23.98.190
Jan 8, 2021 18:28:09.539196014 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.552113056 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.552156925 CET	443	49728	104.23.98.190	192.168.2.4
Jan 8, 2021 18:28:09.552329063 CET	49728	443	192.168.2.4	104.23.98.190
Jan 8, 2021 18:28:45.569504023 CET	49739	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:28:45.618786097 CET	10004	49739	194.5.97.173	192.168.2.4
Jan 8, 2021 18:28:46.125101089 CET	49739	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:28:46.174438000 CET	10004	49739	194.5.97.173	192.168.2.4
Jan 8, 2021 18:28:46.687581062 CET	49739	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:28:46.736856937 CET	10004	49739	194.5.97.173	192.168.2.4
Jan 8, 2021 18:28:52.411062956 CET	49745	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:28:52.461215019 CET	10004	49745	194.5.97.173	192.168.2.4
Jan 8, 2021 18:28:53.109863997 CET	49745	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:28:53.159204960 CET	10004	49745	194.5.97.173	192.168.2.4
Jan 8, 2021 18:28:53.738729000 CET	49745	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:28:53.788064957 CET	10004	49745	194.5.97.173	192.168.2.4
Jan 8, 2021 18:28:59.413294077 CET	49754	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:28:59.462886095 CET	10004	49754	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:00.110843897 CET	49754	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:00.160305977 CET	10004	49754	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:00.798029900 CET	49754	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:00.847595930 CET	10004	49754	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:10.805627108 CET	49759	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:10.855285883 CET	10004	49759	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:11.361377001 CET	49759	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:11.410864115 CET	10004	49759	194.5.97.173	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:29:11.923930883 CET	49759	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:13.954814911 CET	10004	49759	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:18.315542936 CET	49767	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:18.364805937 CET	10004	49767	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:18.877727032 CET	49767	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:18.927046061 CET	10004	49767	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:19.440170050 CET	49767	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:19.490469933 CET	10004	49767	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:28.776222944 CET	49770	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:28.825845957 CET	10004	49770	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:29.331721067 CET	49770	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:29.381279945 CET	10004	49770	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:29.894196987 CET	49770	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:29.943869114 CET	10004	49770	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:34.178714037 CET	49771	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:34.228147030 CET	10004	49771	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:34.738337994 CET	49771	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:34.789946079 CET	10004	49771	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:35.300869942 CET	49771	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:35.350395918 CET	10004	49771	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:37.005249023 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:37.045504093 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.045658112 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:37.273112059 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:37.313086987 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.316292048 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.316313982 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.316323996 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.316410065 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:37.321706057 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:37.361747980 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.361929893 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.410406113 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:37.484163046 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:37.524144888 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.535754919 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.535774946 CET	443	49772	104.23.99.190	192.168.2.4
Jan 8, 2021 18:29:37.535923958 CET	49772	443	192.168.2.4	104.23.99.190
Jan 8, 2021 18:29:42.532982111 CET	49774	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:42.582350969 CET	10004	49774	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:43.082772017 CET	49774	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:43.133642912 CET	10004	49774	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:43.645303011 CET	49774	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:43.694761038 CET	10004	49774	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:50.897908926 CET	49776	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:50.947325945 CET	10004	49776	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:51.458544016 CET	49776	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:51.507946014 CET	10004	49776	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:52.021028042 CET	49776	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:52.070400953 CET	10004	49776	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:59.162651062 CET	49779	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:59.211925030 CET	10004	49779	194.5.97.173	192.168.2.4
Jan 8, 2021 18:29:59.724776030 CET	49779	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:29:59.774046898 CET	10004	49779	194.5.97.173	192.168.2.4
Jan 8, 2021 18:30:00.287364960 CET	49779	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:30:00.336741924 CET	10004	49779	194.5.97.173	192.168.2.4
Jan 8, 2021 18:30:09.765389919 CET	49780	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:30:09.814692020 CET	10004	49780	194.5.97.173	192.168.2.4
Jan 8, 2021 18:30:10.319847107 CET	49780	10004	192.168.2.4	194.5.97.173
Jan 8, 2021 18:30:10.370201111 CET	10004	49780	194.5.97.173	192.168.2.4
Jan 8, 2021 18:30:10.932128906 CET	49780	10004	192.168.2.4	194.5.97.173

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:28:03.163474083 CET	49714	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:03.214591980 CET	53	49714	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:04.288980961 CET	58028	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:04.336911917 CET	53	58028	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:05.430877924 CET	53097	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:05.478806019 CET	53	53097	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:09.182218075 CET	49257	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:09.241352081 CET	53	49257	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:20.362673044 CET	62389	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:20.414274931 CET	53	62389	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:39.259988070 CET	49910	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:39.307970047 CET	53	49910	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:40.389254093 CET	55854	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:40.437110901 CET	53	55854	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:41.574131012 CET	64549	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:41.622072935 CET	53	64549	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:42.536215067 CET	63153	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:42.584234953 CET	53	63153	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:42.894756079 CET	52991	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:42.951260090 CET	53	52991	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:43.436304092 CET	53700	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:43.484148979 CET	53	53700	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:44.710547924 CET	51726	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:44.759284973 CET	53	51726	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:45.472358942 CET	56794	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:45.531147003 CET	53	56794	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:45.629201889 CET	56534	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:45.677192926 CET	53	56534	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:46.523212910 CET	56627	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:46.575221062 CET	53	56627	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:47.326358080 CET	56621	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:47.377506018 CET	53	56621	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:48.163100958 CET	63116	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:48.211038113 CET	53	63116	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:51.745104074 CET	64078	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:51.795805931 CET	53	64078	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:52.290245056 CET	64801	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:52.354598045 CET	53	64801	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:53.013287067 CET	61721	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:53.061291933 CET	53	61721	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:53.892571926 CET	51255	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:53.943299055 CET	53	51255	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:54.863235950 CET	61522	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:54.950402021 CET	53	61522	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:55.505544901 CET	52337	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:55.553472042 CET	53	52337	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:56.052324057 CET	55046	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:56.116507053 CET	53	55046	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:56.476608038 CET	49612	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:56.523276091 CET	49285	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:56.532810926 CET	53	49612	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:56.579338074 CET	53	49285	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:57.673465967 CET	50601	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:57.724289894 CET	53	50601	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:59.313375950 CET	60875	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:59.374864101 CET	53	60875	8.8.8.8	192.168.2.4
Jan 8, 2021 18:28:59.512973070 CET	56448	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:28:59.569612026 CET	53	56448	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:01.338078022 CET	59172	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:01.443854094 CET	53	59172	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:03.978924990 CET	62420	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:04.035427094 CET	53	62420	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:07.487880945 CET	60579	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:07.546094894 CET	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:29:10.748450041 CET	50183	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:10.804574966 CET	53	50183	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:10.995482922 CET	61531	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:11.046228886 CET	53	61531	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:11.463151932 CET	49228	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:11.523710012 CET	53	49228	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:13.144999981 CET	59794	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:14.174741030 CET	59794	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:14.231101990 CET	53	59794	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:18.203933954 CET	55916	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:18.260675907 CET	53	55916	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:20.372546911 CET	52752	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:20.431698084 CET	53	52752	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:21.702075005 CET	60542	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:21.761449099 CET	53	60542	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:28.635936975 CET	60689	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:28.694567919 CET	53	60689	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:34.121220112 CET	64206	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:34.177614927 CET	53	64206	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:36.863101006 CET	50904	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:36.919483900 CET	53	50904	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:39.035324097 CET	57525	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:39.083435059 CET	53	57525	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:42.371758938 CET	53814	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:42.428167105 CET	53	53814	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:43.402868986 CET	53418	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:43.474981070 CET	53	53418	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:49.928546906 CET	62833	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:49.984771967 CET	53	62833	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:53.252557993 CET	59260	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:53.313792944 CET	53	59260	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:53.775106907 CET	49944	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:53.822890043 CET	53	49944	8.8.8.8	192.168.2.4
Jan 8, 2021 18:29:58.927599907 CET	63300	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:29:58.986083984 CET	53	63300	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:09.644856930 CET	61449	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:09.701236010 CET	53	61449	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:15.811732054 CET	51275	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:15.868063927 CET	53	51275	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:24.476016045 CET	63492	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:24.535446882 CET	53	63492	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:24.763263941 CET	58945	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:24.811640978 CET	53	58945	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:25.057379961 CET	60779	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:25.113856077 CET	53	60779	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:26.623346090 CET	64014	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:26.684256077 CET	53	64014	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:30.146119118 CET	57091	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:30.203305960 CET	53	57091	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:34.101454973 CET	55904	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:34.161103964 CET	53	55904	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:35.886343956 CET	52109	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:35.942862988 CET	53	52109	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:41.625237942 CET	54450	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:41.681348085 CET	53	54450	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:45.834404945 CET	49374	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:45.885118961 CET	53	49374	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:46.382834911 CET	50436	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:46.430803061 CET	53	50436	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:47.083993912 CET	62605	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:47.140379906 CET	53	62605	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:48.340528011 CET	54256	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:48.388509989 CET	53	54256	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:51.114455938 CET	52189	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:30:51.162751913 CET	53	52189	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:52.539551020 CET	56131	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:52.587620974 CET	53	56131	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:55.847292900 CET	62992	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:55.895030022 CET	53	62992	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:58.642716885 CET	54432	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:58.701703072 CET	53	54432	8.8.8.8	192.168.2.4
Jan 8, 2021 18:30:59.445573092 CET	57227	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:30:59.496325016 CET	53	57227	8.8.8.8	192.168.2.4
Jan 8, 2021 18:31:04.066267967 CET	58383	53	192.168.2.4	8.8.8.8
Jan 8, 2021 18:31:04.125413895 CET	53	58383	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 18:28:09.182218075 CET	192.168.2.4	8.8.8.8	0xd2b7	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:28:45.472358942 CET	192.168.2.4	8.8.8.8	0x6036	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:28:52.290245056 CET	192.168.2.4	8.8.8.8	0x7ee5	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:28:59.313375950 CET	192.168.2.4	8.8.8.8	0xb1d8	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:10.748450041 CET	192.168.2.4	8.8.8.8	0xb08f	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:18.203933954 CET	192.168.2.4	8.8.8.8	0x10e7	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:28.635936975 CET	192.168.2.4	8.8.8.8	0x2c6d	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:34.121220112 CET	192.168.2.4	8.8.8.8	0x43ab	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:36.863101006 CET	192.168.2.4	8.8.8.8	0x35df	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:42.371758938 CET	192.168.2.4	8.8.8.8	0x7bc2	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:49.928546906 CET	192.168.2.4	8.8.8.8	0x451f	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:58.927599907 CET	192.168.2.4	8.8.8.8	0x27bc	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:09.644856930 CET	192.168.2.4	8.8.8.8	0x2c86	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:15.811732054 CET	192.168.2.4	8.8.8.8	0x85ba	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:24.476016045 CET	192.168.2.4	8.8.8.8	0x4a77	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:25.057379961 CET	192.168.2.4	8.8.8.8	0xc184	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:26.623346090 CET	192.168.2.4	8.8.8.8	0x4f	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:30.146119118 CET	192.168.2.4	8.8.8.8	0x241d	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:34.101454973 CET	192.168.2.4	8.8.8.8	0x1b2a	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:35.886343956 CET	192.168.2.4	8.8.8.8	0x8742	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:41.625237942 CET	192.168.2.4	8.8.8.8	0xd7b1	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:47.083993912 CET	192.168.2.4	8.8.8.8	0x9c23	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:48.340528011 CET	192.168.2.4	8.8.8.8	0x2b66	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:52.539551020 CET	192.168.2.4	8.8.8.8	0x22a9	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:58.642716885 CET	192.168.2.4	8.8.8.8	0x918d	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:59.445573092 CET	192.168.2.4	8.8.8.8	0xdcb2	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:31:04.066267967 CET	192.168.2.4	8.8.8.8	0xa051	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 8, 2021 18:28:09.241352081 CET	8.8.8.8	192.168.2.4	0xd2b7	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:28:09.241352081 CET	8.8.8.8	192.168.2.4	0xd2b7	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:28:45.531147003 CET	8.8.8.8	192.168.2.4	0x6036	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:28:52.354598045 CET	8.8.8.8	192.168.2.4	0x7ee5	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:28:59.374864101 CET	8.8.8.8	192.168.2.4	0xb1d8	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:10.804574966 CET	8.8.8.8	192.168.2.4	0xb08f	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:18.260675907 CET	8.8.8.8	192.168.2.4	0x10e7	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:28.694567919 CET	8.8.8.8	192.168.2.4	0x2c6d	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:34.177614927 CET	8.8.8.8	192.168.2.4	0x43ab	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:36.919483900 CET	8.8.8.8	192.168.2.4	0x35df	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:36.919483900 CET	8.8.8.8	192.168.2.4	0x35df	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:42.428167105 CET	8.8.8.8	192.168.2.4	0x7bc2	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:49.984771967 CET	8.8.8.8	192.168.2.4	0x451f	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:29:53.313792944 CET	8.8.8.8	192.168.2.4	0x7754	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 8, 2021 18:29:58.986083984 CET	8.8.8.8	192.168.2.4	0x27bc	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:09.701236010 CET	8.8.8.8	192.168.2.4	0x2c86	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:15.868063927 CET	8.8.8.8	192.168.2.4	0x85ba	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:24.535446882 CET	8.8.8.8	192.168.2.4	0x4a77	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:25.113856077 CET	8.8.8.8	192.168.2.4	0xc184	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:25.113856077 CET	8.8.8.8	192.168.2.4	0xc184	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:26.684256077 CET	8.8.8.8	192.168.2.4	0x4f	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:26.684256077 CET	8.8.8.8	192.168.2.4	0x4f	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:30.203305960 CET	8.8.8.8	192.168.2.4	0x241d	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:34.161103964 CET	8.8.8.8	192.168.2.4	0x1b2a	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:34.161103964 CET	8.8.8.8	192.168.2.4	0x1b2a	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:35.942862988 CET	8.8.8.8	192.168.2.4	0x8742	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 8, 2021 18:30:41.681348085 CET	8.8.8.8	192.168.2.4	0xd7b1	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:47.140379906 CET	8.8.8.8	192.168.2.4	0x9c23	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:48.388509989 CET	8.8.8.8	192.168.2.4	0x2b66	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:48.388509989 CET	8.8.8.8	192.168.2.4	0x2b66	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:52.587620974 CET	8.8.8.8	192.168.2.4	0x22a9	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:58.701703072 CET	8.8.8.8	192.168.2.4	0x918d	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:59.496325016 CET	8.8.8.8	192.168.2.4	0xdcb2	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:30:59.496325016 CET	8.8.8.8	192.168.2.4	0xdcb2	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:31:04.125413895 CET	8.8.8.8	192.168.2.4	0xa051	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 8, 2021 18:28:09.406292915 CET	104.23.98.190	443	192.168.2.4	49728	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 8, 2021 18:29:37.316323996 CET	104.23.99.190	443	192.168.2.4	49772	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 8, 2021 18:30:25.281522989 CET	104.23.99.190	443	192.168.2.4	49784	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

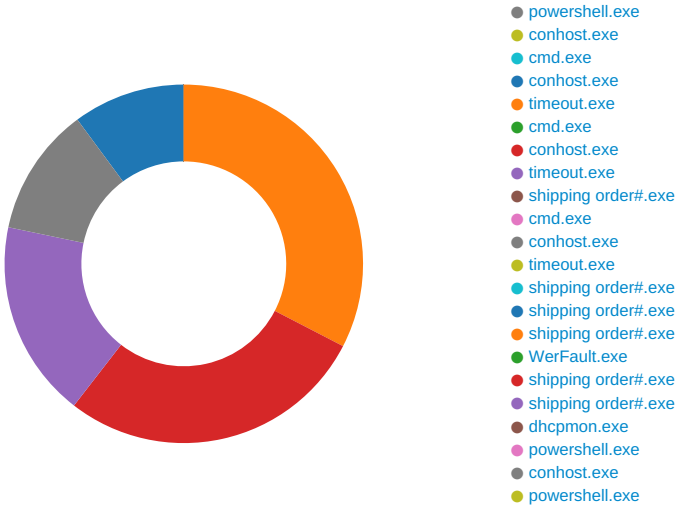
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 8, 2021 18:30:26.827495098 CET	104.23.98.190	443	192.168.2.4	49785	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 8, 2021 18:30:34.288294077 CET	104.23.99.190	443	192.168.2.4	49787	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 8, 2021 18:30:48.537064075 CET	104.23.98.190	443	192.168.2.4	49793	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 8, 2021 18:30:59.593247890 CET	104.23.99.190	443	192.168.2.4	49798	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

- shipping order#.exe
- powershell.exe
- conhost.exe
- powershell.exe
- powershell.exe
- conhost.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: shipping order#.exe PID: 5884 Parent PID: 1284

General

Start time:	18:27:59
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\shipping order#.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping order#.exe'
Imagebase:	0xc20000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.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	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\50bacdd5-1381-4848-995e-cb76453c6468	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW

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	6D3DCF06	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	6D3DCF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe	0	524288	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 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 12 2a f8 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 70 28 00 00 8e 02 00 00 00 00 00 8e 8f 28 00 00 20 00 00 00 a0 28 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 2b 00 00 02 00 00 ff ad 28 00 02 00 40 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....*._.......... ....p(...........(.. ....(...@.. ....`+....... (...@................................	success or wait	6	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C22DD66	CopyFileW

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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D39D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D39D72F	unknown
C:\Users\user\Desktop\shipping order#.exe	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Users\user\Desktop\shipping order#.exe	unknown	512	success or wait	1	6D39D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6C225F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6C225F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6C225F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6C225F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6C225F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6C225F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	<Unknown>	unicode	C:\Users\user\Desktop\shipping order#.exe	success or wait	1	6C22646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\ Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe	dword	0	success or wait	1	6C22C075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	shell	unicode	explorer.exe,"C:\Users\user\Desktop\shipping order#.exe"	success or wait	1	6C22646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	shipping order#.exe	unicode	C:\Users\user\Desktop\shipping order#.exe	success or wait	1	6C22646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\shipping order#.exe	dword	0	success or wait	1	6C22C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6C22C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6C22C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6C22C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6C22C075	RegSetValueExW

Analysis Process: powershell.exe PID: 5796 Parent PID: 5884

General

Start time:	18:28:04
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force
Imagebase:	0x380000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e04p2qly.o2t.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fraa5aiu.gcp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\Documents\20210108	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.tt6CRrQ7.20210108182806.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e04p2qly.o2t.ps1	success or wait	1	6C226A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fraa5aiu.gcp.psm1	success or wait	1	6C226A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e04p2qly.o2t.ps1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fraa5aiu.gcp.psm1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.tt6CRrQ7.20210108182806.txt	unknown	3	ef bb bf	...	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.tt6CRrQ7.20210108182806.txt	unknown	735	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 38 31 38 32 38 33 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 30 31 31 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210108182836..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0d 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	2	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	2	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2242	2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 4e 65 77 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 1c 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 46 69 6c 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 00 00 00 00 79 f0 c9 a8 15 a0 d5 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 64 31 17 00 00 00 08 00 00 00 44 65 73 63 72 69 62 65 02 00 00 00 11 00 00 00 47 65 74 2d 54 65 73 74 44 72 69 76 65 49 74 65 6d 02 00 00 00 0b 00 00 00 4e 65 77 2d 46 69 78	-AppLockerPolicy.....New-AppLockerPolicy.....Get-AppLockerPolicy.....Get-AppLockerFileInformation.....y.....I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fix	success or wait	2	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 76 fa 78 15 a0 d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....v.x....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D3C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6D3C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C221B4F	ReadFile

Analysis Process: conhost.exe PID: 4984 Parent PID: 5796

General

Start time:	18:28:05
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: powershell.exe PID: 5128 Parent PID: 5884

General

Start time:	18:28:05
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force
Imagebase:	0x380000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6D3DCF06	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	6D3DCF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C185B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C185B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_x2khrpam.ug2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yf4s2bry.3jw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.Laubqkk7.20210108182807.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	3	6C221E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_x2khrpam.ug2.ps1	success or wait	1	6C226A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yf4s2bry.3jw.psm1	success or wait	1	6C226A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_x2khrpam.ug2.ps1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yf4s2bry.3jw.psm1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.Laubqkk7.20210108182807.txt	unknown	3	ef bb bf	...	success or wait	1	6C221B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.Laubqkk7.20210108182807.txt	unknown	735	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 38 31 38 32 38 33 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 30 31 31 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210108182839..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	3	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0d 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	2	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	2	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 76 fa 78 15 a0 d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....v.x....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D3C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6D3C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	2	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: powershell.exe PID: 4944 Parent PID: 5884

General

Start time:	18:28:05
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force
Imagebase:	0x380000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pilnwesf.xu0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_harhvbow.ned.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.nGv+RGBh.20210108182808.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pilnwesf.xu0.ps1	success or wait	1	6C226A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_harhvbow.ned.psm1	success or wait	1	6C226A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pilnwesf.xu0.ps1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_harhvbow.ned.psm1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.nGv+RGBh.20210108182808.txt	unknown	3	ef bb bf	...	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.nGv+RGBh.20210108182808.txt	unknown	735	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 38 31 38 32 38 34 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 30 31 31 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210108182847..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D3C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6D3C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C221B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: conhost.exe PID: 6684 Parent PID: 5128

General

Start time:	18:28:05
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6828 Parent PID: 4944

General

Start time:	18:28:06
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6836 Parent PID: 5884

General

Start time:	18:28:06
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\shipping order#.exe' -Force
Imagebase:	0x380000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_brge2zcm.hwd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czsau0n1.mqj.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\Documents\20210108\PowerShell_transcr ipt.701188.ONgqdUkt.20210108182809.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_brge2zcm.hwd.ps1	success or wait	1	6C226A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czsau0n1.mqj.psm1	success or wait	1	6C226A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_brge2zcm.hwd.ps1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_czsau0n1.mqj.psm1	unknown	1	31	1	success or wait	1	6C221B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcr ipt.701188.ONgqdUkt.20210108182809.txt	unknown	3	ef bb bf	...	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210108\PowerShell_transcript.701188.ONgqdUkt.20210108182809.txt	unknown	681	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 38 31 38 32 38 34 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 30 31 31 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210108182848..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D3C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6D3C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: conhost.exe PID: 6900 Parent PID: 6836

General

Start time:	18:28:06
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6996 Parent PID: 5884

General

Start time:	18:28:09
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 7132 Parent PID: 6996

General

Start time:	18:28:10
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6948 Parent PID: 6996

General

Start time:	18:28:10
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x30000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Analysis Process: cmd.exe PID: 2460 Parent PID: 5884

General

Start time:	18:28:13
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 7160 Parent PID: 2460

General

Start time:	18:28:13
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6eb840000
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: timeout.exe PID: 5136 Parent PID: 2460

General

Start time:	18:28:13
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x30000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: shipping order#.exe PID: 5812 Parent PID: 3424

General

Start time:	18:28:16
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\shipping order#.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping order#.exe'
Imagebase:	0x310000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: cmd.exe PID: 4176 Parent PID: 5884

General

Start time:	18:28:20
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6812 Parent PID: 4176

General

Start time:	18:28:21
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 7124 Parent PID: 4176

General

Start time:	18:28:21
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x30000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: shipping order#.exe PID: 6440 Parent PID: 3424

General

Start time:	18:28:24
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\shipping order#.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping order#.exe'
Imagebase:	0x490000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: shipping order#.exe PID: 6648 Parent PID: 5884

General

Start time:	18:28:29
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\shipping order#.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\shipping order#.exe
Imagebase:	0xe60000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
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: 00000016.00000002.953347947.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.953347947.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.953347947.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: shipping order#.exe PID: 6476 Parent PID: 3424

General

Start time:	18:28:32
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\shipping order#.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping order#.exe'
Imagebase:	0x120000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: WerFault.exe PID: 5824 Parent PID: 5884

General

Start time:	18:28:38
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5884 -s 2396
Imagebase:	0xac0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: shipping order#.exe PID: 408 Parent PID: 3424

General

Start time:	18:28:41
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\shipping order#.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping order#.exe'
Imagebase:	0x530000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: shipping order#.exe PID: 5700 Parent PID: 3424

General

Start time:	18:28:49
Start date:	08/01/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe'
Imagebase:	0x8b0000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs

Analysis Process: dhcpmon.exe PID: 5392 Parent PID: 3424

General

Start time:	18:29:03
Start date:	08/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'

Imagebase:	0x9e0000
File size:	2818048 bytes
MD5 hash:	A916070DF947A28EA73074C080189D35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs

Analysis Process: powershell.exe PID: 1836 Parent PID: 5812

General

Start time:	18:29:16
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force
Imagebase:	0x380000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6308 Parent PID: 1836

General

Start time:	18:29:16
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2848 Parent PID: 5812

General

Start time:	18:29:16
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order#.exe' -Force
Imagebase:	0x380000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis