ID: 337538
Sample Name: shipping order.exe
Cookbook: default.jbs
Time: 18:30:19
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

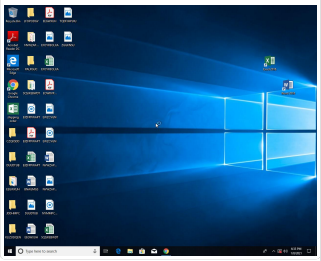
Analysis Report shipping order.exe

Overview

General Information

Sample Name:	shipping order.exe
Analysis ID:	337538
MD5:	b87925c7eb04ed..
SHA1:	cff199d7a3b2ecb..
SHA256:	8daa3b16b15dd5..
Tags:	Endurance exe NanoCore RAT

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

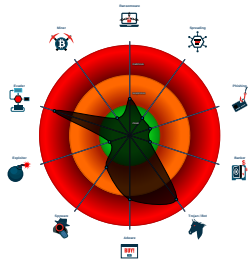
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Powershell adding …
- Yara detected Nanocore RAT
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Connects to a pastebin service (like…
- Creates an undocumented autostart …
- Creates autostart registry keys with …

Classification



Startup

- **System is w10x64**
- shipping order.exe (PID: 5316 cmdline: 'C:\Users\user\Desktop\shipping order.exe' MD5: B87925C7EB04ED03B7D1B9A5A39358D8)
  - powershell.exe (PID: 1000 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: 4668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 768 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: 5996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4724 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: 5680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4600 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: 5896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6292 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6464 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 6728 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6820 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 1688 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6460 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - shipping order.exe (PID: 5732 cmdline: C:\Users\user\Desktop\shipping order.exe MD5: B87925C7EB04ED03B7D1B9A5A39358D8)
  - WerFault.exe (PID: 5960 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5316 -s 2616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- shipping order.exe (PID: 6696 cmdline: 'C:\Users\user\Desktop\shipping order.exe' MD5: B87925C7EB04ED03B7D1B9A5A39358D8)
  - 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: 5144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- shipping order.exe (PID: 1624 cmdline: 'C:\Users\user\Desktop\shipping order.exe' MD5: B87925C7EB04ED03B7D1B9A5A39358D8)
- shipping order.exe (PID: 5860 cmdline: 'C:\Users\user\Desktop\shipping order.exe' MD5: B87925C7EB04ED03B7D1B9A5A39358D8)
- shipping order.exe (PID: 6892 cmdline: 'C:\Users\user\Desktop\shipping order.exe' MD5: B87925C7EB04ED03B7D1B9A5A39358D8)
- shipping order.exe (PID: 6436 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order.exe' MD5: B87925C7EB04ED03B7D1B9A5A39358D8)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "311.10.11.15"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001E.00000002.551692234.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001E.00000002.551692234.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001E.00000002.551692234.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000E.00000002.610896379.0000000004C82000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x102dd:$x1: NanoCore.ClientPluginHost • 0x430fd:$x1: NanoCore.ClientPluginHost • 0x75d1d:$x1: NanoCore.ClientPluginHost • 0x1031a:$x2: IClientNetworkHost • 0x4313a:$x2: IClientNetworkHost • 0x75d5a:$x2: IClientNetworkHost • 0x13e4d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x46c6d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7988d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.610896379.0000000004C82000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
30.2.shipping order.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
30.2.shipping order.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
30.2.shipping order.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
30.2.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

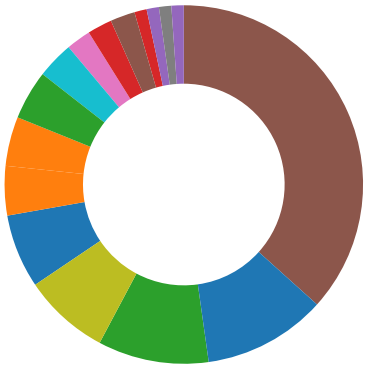
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Powershell adding suspicious path to exclusion list

Signature Overview



Click to jump to signature section

- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

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

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:

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

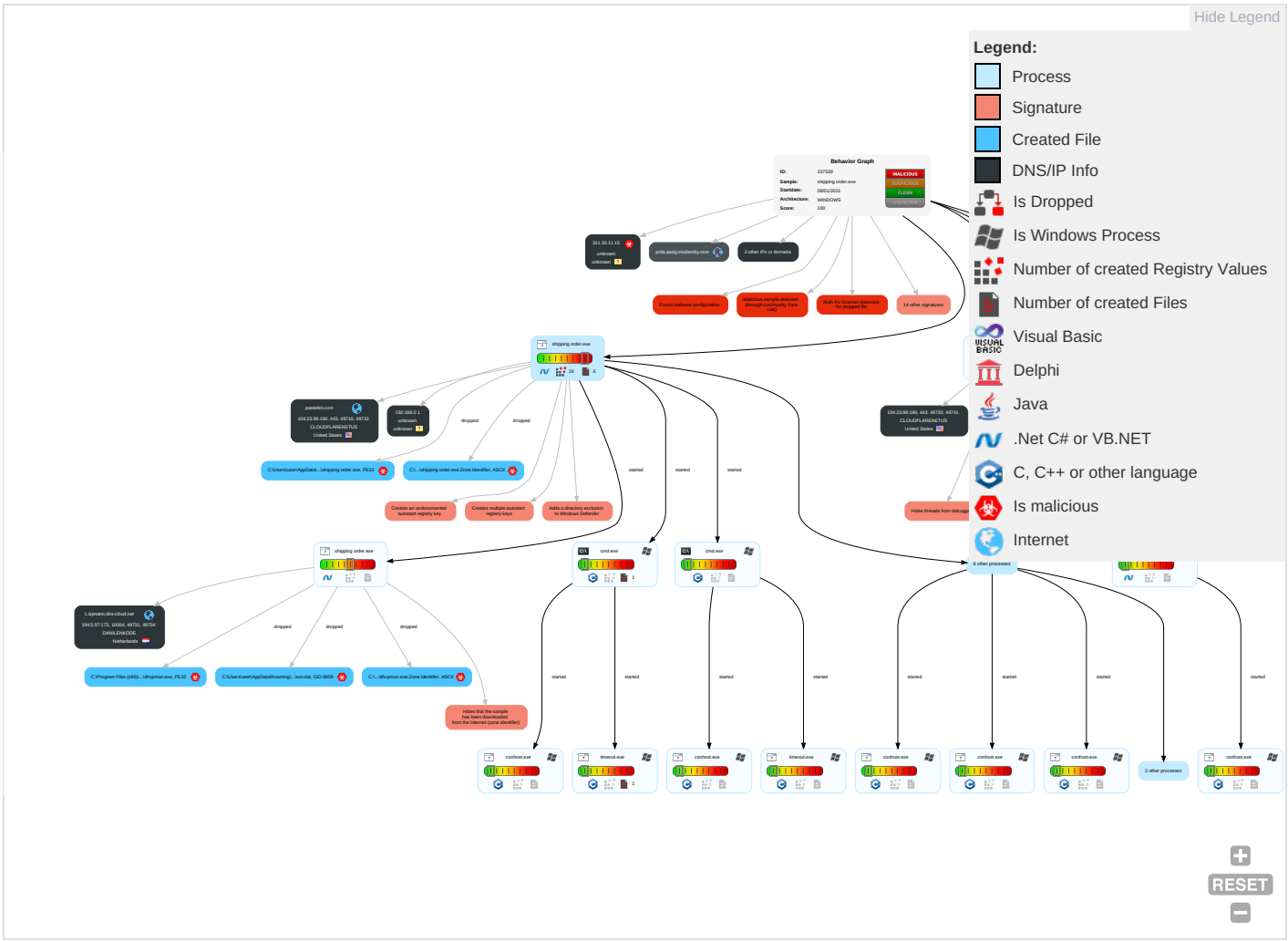
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 1 1	Startup Items 1	Startup Items 1	Masquerading 2	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Web Service 1

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

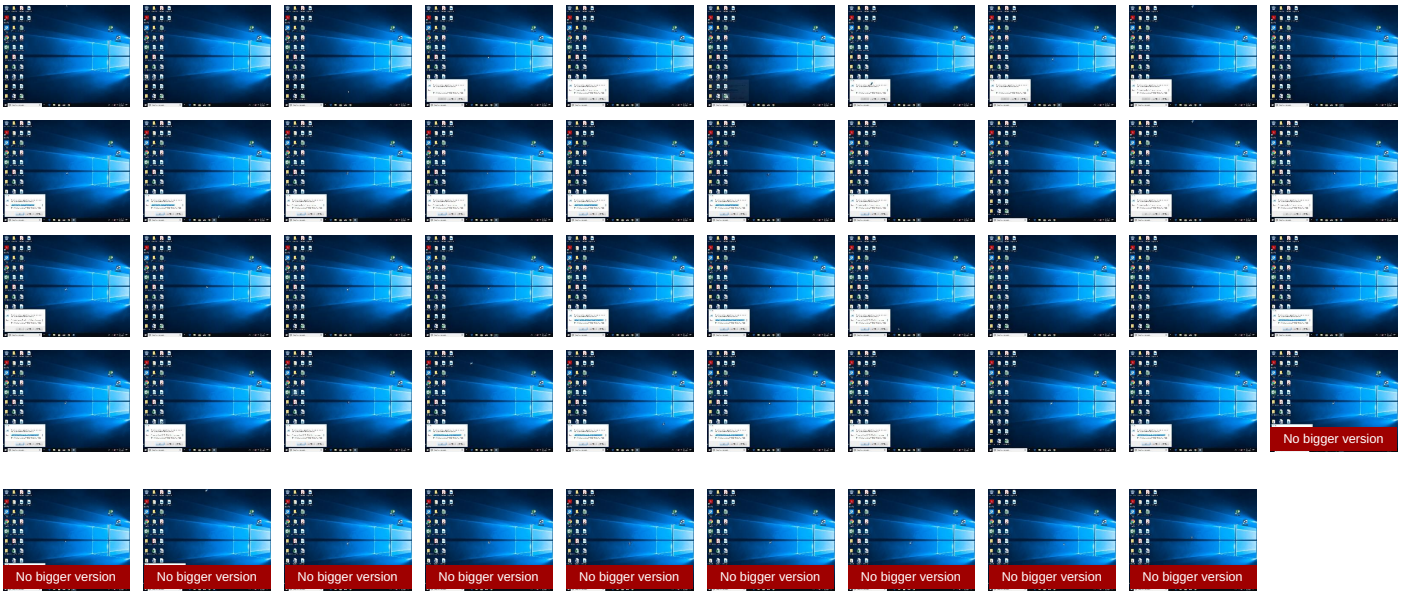
Behavior Graph



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	35%	Virustotal		Browse
shipping order.exe	30%	ReversingLabs	Win32.Trojan.Wacatac	
shipping order.exe	100%	Joe Sandbox ML		

Dropped Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.pngt	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	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://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png$6	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://pastebin.com4	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		unknown
pastebin.com	104.23.99.190	true	false		high

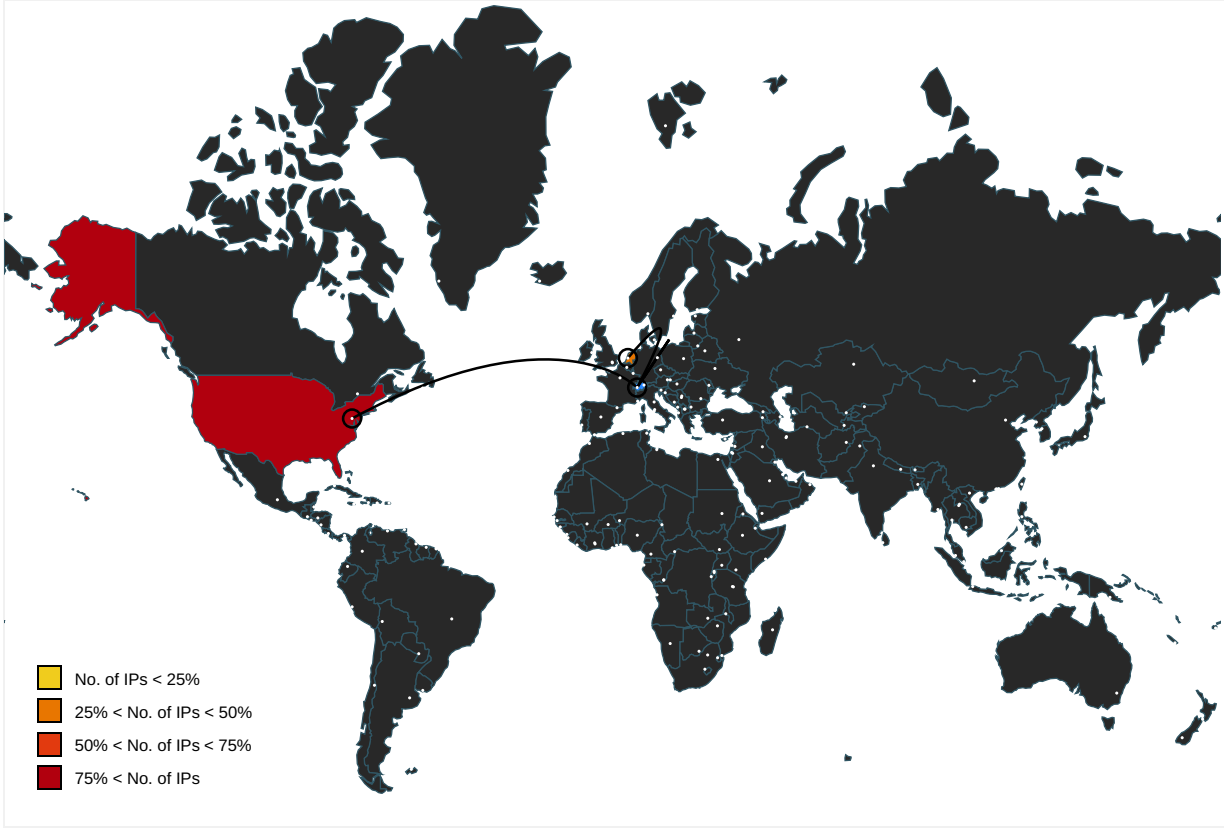
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.pngt	powershell.exe, 00000001.00000002.605929285.000000000488D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Pester/Pestert	powershell.exe, 00000001.00000002.605929285.000000000488D000.00000004.00000001.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000006.00000002.631313562.0000000005C84000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester$6	powershell.exe, 00000003.00000002.606076102.000000000495E000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000006.00000002.603137277.0000000004D5E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000001.00000002.605929285.000000000488D000.00000004.00000001.sdmp, powershell.exe, 00000003.00000002.606076102.000000000495E000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.605732034.000000000531E000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.603137277.0000000004D5E000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000006.00000002.603137277.0000000004D5E000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000001.00000003.505791219.0000000005105000.00000004.00000001.sdmp, powershell.exe, 00000005.00000003.531194458.0000000005B92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pastebin.com/raw/W63zsRav	shipping order.exe, 0000001D.00000002.624812497.000000000338A000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000001.00000002.605929285.000000000488D000.00000004.00000001.sdmp, powershell.exe, 00000003.00000002.606076102.000000000495E000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.605732034.000000000531E000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.603137277.0000000004D5E000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000006.00000002.631313562.0000000005C84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000006.00000002.631313562.0000000005C84000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000006.00000002.631313562.0000000005C84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png$6	powershell.exe, 00000003.00000002.606076102.000000000495E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000006.00000002.631313562.0000000005C84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pastebin.com4	shipping order.exe, 00000000.00000002.629479307.0000000003550000.00000004.00000001.sdmp, shipping order.exe, 0000000E.00000002.532866722.000000000371A000.00000004.00000001.sdmp, shipping order.exe, 0000001B.00000002.623796584.000000000362A000.00000004.00000001.sdmp, shipping order.exe, 0000001D.00000002.624812497.00000000338A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html$6	powershell.exe, 00000003.00000002.606076102.000000000495E000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	shipping order.exe, 00000000.00000002.611055849.0000000002EB1000.00000004.00000001.sdmp, powershell.exe, 00000001.00000002.601882305.0000000004751000.00000004.00000001.sdmp, powershell.exe, 00000003.00000002.600388750.0000000004821000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.600934151.00000000051E1000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.597635539.0000000004C21000.00000004.00000001.sdmp, shipping order.exe, 0000000E.00000002.484012193.0000000030D1000.00000004.00000001.sdmp, shipping order.exe, 0000001B.00000002.605222974.00000002FE1000.00000004.00000001.sdmp, shipping order.exe, 0000001D.00000002.607170263.0000000002D41000.00000004.00000001.sdmp, shipping order.exe, 00000022.00000002.604939441.0000000002F71000.00000004.00000001.sdmp	false		high
http://pastebin.com	shipping order.exe, 00000000.00000002.629763939.0000000003563000.00000004.00000001.sdmp, shipping order.exe, 0000000E.00000002.535270665.0000000003783000.00000004.00000001.sdmp, shipping order.exe, 0000001B.00000002.624981836.0000000003693000.00000004.00000001.sdmp, shipping order.exe, 0000001D.00000002.625714191.00000000033F3000.00000004.00000001.sdmp	false		high
http://https://pastebin.com	shipping order.exe, 00000000.00000002.629479307.0000000003550000.00000004.00000001.sdmp, shipping order.exe, 0000000E.00000002.532866722.000000000371A000.00000004.00000001.sdmp, shipping order.exe, 0000001B.00000002.623796584.000000000362A000.00000004.00000001.sdmp, shipping order.exe, 0000001D.00000002.624812497.00000000338A000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.htmlt	powershell.exe, 00000001.00000002.605929285.000000000488D000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000006.00000002.603137277.0000000004D5E000.00000004.00000001.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
311.10.11.15	unknown	unknown		unknown	unknown	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337538
Start date:	08.01.2021
Start time:	18:30:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shipping order.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@55/23@26/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 93.2% • Quality standard deviation: 8.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 13.64.90.137, 23.210.248.85, 51.11.168.160, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 51.103.5.159, 20.54.26.129, 40.126.1.166, 40.126.1.130, 20.190.129.17, 20.190.129.160, 40.126.1.145, 40.126.1.142, 40.126.1.128, 20.190.129.130, 13.88.21.125, 40.88.32.150, 168.61.161.212, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • 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 exceeded maximum capacity and may have missing disassembly code. • 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
18:31:23	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\shipping order.exe
18:31:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run shipping order.exe C:\Users\user\Desktop\shipping order.exe
18:31:40	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\shipping order.exe
18:31:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run shipping order.exe C:\Users\user\Desktop\shipping order.exe
18:31:57	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\shipping order.exe
18:32:09	API Interceptor	456x Sleep call for process: shipping order.exe modified
18:32:11	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:32:27	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run dhcpmon.exe C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:32:35	API Interceptor	155x Sleep call for process: powershell.exe modified
18:32:36	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run dhcpmon.exe C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:32:47	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
194.5.97.173	shipping order#.exe	Get hash	malicious	Browse	
104.23.98.190	b095b966805abb7df4ffddf183def880.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	E1Q0TjeN32.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	6YCl3ATKJw.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	Hjnb15Nuc3.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	JDgYMW0LHW.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	4av8Sn32by.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
	T6OcyQsUsY.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	1KlTgJnGbl.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
	PbTwrajNMX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	22NO7gVJ7r.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	rE7DwszvrX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VjPHSJkwr6.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	wf86K0dpOP.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VrR9J0FnSG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	6C1MYmrVl1.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	aTZQZVVriQ.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
1.ispnano.dns-cloud.net	shipping order#.exe	Get hash	malicious	Browse	• 194.5.97.173
pastebin.com	shipping order#.exe	Get hash	malicious	Browse	• 104.23.98.190
	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
	httpscdndiscordappcomattachments785319022966997035791667564027052052aGBWK3jv8vMhTU3.exe	Get hash	malicious	Browse	• 104.23.99.190
	sz.exe	Get hash	malicious	Browse	• 104.23.99.190

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	shipping order#.exe	Get hash	malicious	Browse	• 194.5.97.173
	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
CLOUDFLARENETUS	shipping order#.exe	Get hash	malicious	Browse	• 104.23.98.190
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
CLOUDFLARENETUS	shipping order#.exe	Get hash	malicious	Browse	• 104.23.98.190
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	shipping order#.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	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
	DSj7ak0N6I.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Setup_6953.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):	2814976
Entropy (8bit):	3.789835376583671
Encrypted:	false
SSDEEP:	24576:H+x252KxvT7AGiQo6wvooXWR6p7fsqMPDTl2LRVa4IdO3Y9RpQ7aw7L9gLWg4cTg:uce6kaPDToi4IdWY67awV
MD5:	B87925C7EB04ED03B7D1B9A5A39358D8
SHA1:	CFF199D7A3B2ECB1D5A6C2BA48DE92901789CFDA
SHA-256:	8DAA3B16B15DD52FFB99EB0644B52712D889FE9528F8633DD16B4B405B017130
SHA-512:	0E9ACF9FDE99FC48DDA2C878474D53716F4D574B2E488B4A80B96A9692F97A620EFE9E14C7E1AB5C74C85808D2D38EF465CB489E210D0FE92DC1A3E6B35CF18
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....'._.....d(.....(.. ....(...@.. .....`+....._).. .@.....(.W.....(.P.....h(.@....@+..... ..... ..H.....text....b(.. ...d(..... ..`.rsrc...P.....(.....f(.....@..@.reloc.....@+.....*.....@..B.....(.....H.....'.....|.....*.r...p.....r...p.....r...p.....s.....s}.....*6.~....o....&**....(....*~~....:....(....s%.....~....*. ....*.....90...(....9.....r.!p....((...()...*.....(*...*....*2rZ.!p.(....*2r..!p.(....*2r..!p.(....*2r.!p.(....*2r..!p.(....*2r@.!p.(....*2rj.!p.(....*2r..!p.(....*2r..!p.(....*2r.!p.(....*2r..!p.(....*2r2.!p.(....*2rj.!p.(....*2r..!p.(....*2r..!p.(....*2r..!p.(....*2r,.!p

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\WERE82.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):	8426
Entropy (8bit):	3.6922006885436494
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNikr6OV6YI3SUr9jgmfZDS1Cpr+89b+nJsfcqm:RrlsNi46i6YISUr9jgmfdS6+nifg
MD5:	8EC773920127CC70F684748F39D8DAAD
SHA1:	CD5FD0A9A8ABE65ED06188888F64CE791B024680
SHA-256:	5A6DDEDFC55668F4A559468FAE73D73FD3D5ADCE762DBA4E8B95111345164B81

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE82.tmp.WERInternalMetadata.xml	
SHA-512:	E1F1855E0DAB014B73C3258C5CDA6B6F5301CBC659D63EE45DF17CB68B1AB970EBCAC9F212166ECC2C16DA020A2689CAF8CD7264CF9741EAA20430A8F079E E2
Malicious:	false
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.>.5.3.1.6.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE9A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Jan 9 02:33:24 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	338103
Entropy (8bit):	3.7458438738028703
Encrypted:	false
SSDEEP:	3072:9PG70bjd+pwlutLhDt9gIOgF51/kFyn90WcUCgUjTbDe9ogzalRXbUSTgg0:I0kpLB9RpDyo4TjrDgYRXbur
MD5:	2EC60CA587726F042C3CD401E0EF5692
SHA1:	374DE035094A361FC7B99378A83EC2C98B6C06C5
SHA-256:	F64A3E5E34AD3C009B0834F8446BE1B17F0721457320F65FBBD74800BD805A24
SHA-512:	C15532FDEF826F31925000128DFFD33B8791A510BCD55E6E6F5B4688223EFF1CE1958D5255208DECFBCB579D7E480CC75AB4D9A57B62FBF099FBC46F5A16A8 8
Malicious:	false
Preview:	MDMP..... ....._.....U.....B.....1.....GenuineIntelW.....T.....q.._.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .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:	dropped
Size (bytes):	11132
Entropy (8bit):	4.965005105667347
Encrypted:	false
SSDEEP:	192:cdcU6Clib41xoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smc/:cib4kBVoGIpN6KQkj2Wkjh4iUxQedNYH
MD5:	C6B0EDFC1B773A7775BEAE3A2A814653
SHA1:	7A09CD0BFF6B2BC665A2ECAC3144D65ABE89557A
SHA-256:	E576F7164C30F8660E7AD2BF38D312E25812A70481BBB7F2172A3C490AADFB2B
SHA-512:	FE668205C21F0C642DEB54F8F49AD9F8E356A15791C4D9357B7EEC70D11FA0DDB45648600B75887B800021494922E662F0655EC12E5F55C1788DC5F9459B0241
Malicious:	false
Preview:	PSMODULECACHE.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSourc e.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....I mport-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D..8.....C:\Program Files (x8 6)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation..... ..Invoke-OperationValidation.....PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1..... ..Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command..

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ba2ypcd4.fal.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_dgie3wtq.dtl.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_f13zkzre.whv.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_gz3jep32.ccp.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_jtqpnezb.p40.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_sdzbntk1.vuf.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_tiyw5ytt.diz.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_ydljvnmn.obz.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\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:ljRP:X
MD5:	96E6C1FC9F7B152A7AB7EAFEE82C876D
SHA1:	674DBA932D7804065B1391A4D9BD7B6F4D60C1C8
SHA-256:	E4C81288F17ED0B30D27269F9AA7EC6092DF62FEBE87398176B6BF151E23C8FD
SHA-512:	0EBAF091488C3478F50D94B33CE69A6D82C104FB874257754AB29CB8D0D2417EE57D6C3D984BA3A0D2E8B845F4CBCD59C243F3770ADF76E485101983DFBA35 F
Malicious:	**true**
Preview:	.Rv.F..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):	2814976
Entropy (8bit):	3.789835376583671
Encrypted:	false
SSDEEP:	24576:H+x252KxvT7AGiQo6wvooXWR6p7fsqMPDTl2LRVa4IdO3Y9RpQ7aw7L9gLWg4cTg:uce6kaPDToi4IdWY67awV
MD5:	B87925C7EB04ED03B7D1B9A5A39358D8
SHA1:	CFF199D7A3B2ECB1D5A6C2BA48DE92901789CFDA
SHA-256:	8DAA3B16B15DD52FFB99EB0644B52712D889FE9528F8633DD16B4B405B017130
SHA-512:	0E9ACF9FDE99FC48DDA2C878474D53716F4D574B2E488B4A80B96A9692F97A620EFE9E14C7E1AB5C74C85808D2D38EF465CB489E210D0FE92DC1A3E6B35CF18
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....'._.....d(.....(.. ....(...@.. .....`+....._).. .@.....(.W.....(.P.....h(.@....@+..... ..... ..H.....text....b(.. ...d(..... ..`.rsrc...P.....(.....f(.....@..@.reloc.....@+.....*.....@..B.....(.....H.....'....|.....*.r...p.....r...p.....r...p.....s.....s}.....*6.~....o....&**....(....*~~....:...(....s%.....~....*. ....*.....90...(....9.....r.!p....((...()...*.....(*...*....*2rZ.!p.(....*2r..!p.(....*2r..!p.(....*2r..!p.(....*2r..!p.(....*2r..!p.(....*2r@.!p.(....*2rj.!p.(....*2r..!p.(....*2r..!p.(....*2r.!p.(....*2r.!p.(....*2r2.!p.(....*2rj.!p.(....*2r..!p.(....*2r..!p.(....*2r..!p.(....*2r,.!p

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.579569.7jdhcRPS.20210108183127.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):	856
Entropy (8bit):	5.2862634087649925
Encrypted:	false
SSDEEP:	24:BxSAvDvBBMQG+x2DOXUWeSuVbrWWHjeTKKjX4CIym1ZJXTuVbj:BZ7v/dZoO+SmbCWqDYB1Z1mbj
MD5:	60249CEB6B2D32ED65B2A4C6974C0014
SHA1:	92F686A6F8321E10ADE8C64E7B64513F6AA4C4A8
SHA-256:	0807E171D8C560105B33F3C3A460186574B50A0CA80C9E0C0C244DCF0035E154
SHA-512:	EF91EAA398A8B6DBDABF2D9C3B2DA0A94CB6183E29995568C2CA4CE4084F43EB709D391B656BCC5E765434AA4B97A82574E9C92A54254F339F55FE1E5B9B0CD2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108183203..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (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: 4600..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: 20210108183203..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\shipping order.exe -Force..

C:\Users\user\Documents\20210108\PowerShell_transcript.579569.BT05d3d0.20210108183125.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):	963
Entropy (8bit):	5.3050186988842345
Encrypted:	false
SSDEEP:	24:BxSAQDvBBMQG+x2DOXUWeSuvuVM5rWhHjeTKKjX4CIym1ZJXTuvuVM5j:BZ8v/dZoO+SsuaChqDYB1Z1suaj

C:\Users\user\Documents\20210108\PowerShell_transcript.579569.BT05d3d0.20210108183125.txt	
MD5:	7B01E2AC36A3A397BBC6AF73914CB3FF
SHA1:	16E2AAE1940290466BEBA7E3D441D6B4BB8B532A
SHA-256:	23AFD81F7ED132506BA8BD66798D1D2467BE4F9E4409991565ADB21520F41B98
SHA-512:	803109B0B6BB9A58A5B20797BEAFCB5AA2214818866270D2078B4ADE9B6B69624BFD569E4FB3B120DC68E0F57D047B1CAE1311B7E6BB4C72A35AC20A515D937E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108183202..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (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: 768..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: 20210108183203..**********..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.579569.c+4r7aH8.20210108183126.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):	964
Entropy (8bit):	5.306681687338691
Encrypted:	false
SSDEEP:	24:BxSA9DvBBMQG+x2DOXUWeSuvuVM5rWFHjeTKKjX4CIym1ZJXYuvuVM5j:BZFv/dZoO+SsuaCFqDYB1ZOsuaj
MD5:	300C91800B2E2CB773080AEBB3B6B874
SHA1:	CE1346830CB70E5097D64D61FB625903C3022CE8
SHA-256:	5E84C5E2696DF2125EFD5D84A8986CF89032694300A6C373E10DC39CE176931D
SHA-512:	EE5C159307E4B91AFD3E85A61D79F20030523AF3F80328E10D5D6D8F89F6F2854F5E7B3604FD98B57856A5EC372989445963D251CD9F33614E8617532FE6632F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108183205..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (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: 4724..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: 20210108183208..**********..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.579569.hrKQHeuP.20210108183125.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):	964
Entropy (8bit):	5.298122737331953
Encrypted:	false
SSDEEP:	24:BxSAvDvBBMQG+x2DOXUWeSuvuVM5rWbHjeTKKjX4CIym1ZJXzuvuVM5j:BZ7v/dZoO+SsuaCbqDYB1ZRsuaj
MD5:	8749A289EB6E272172CDEE32BEA16BE8
SHA1:	B3D5C116852223D6355DED220CC0CC601B2364E7
SHA-256:	4853F9119CB3554FAAA18B48116A808F2921E36E85501A49EC74527CD44990AA
SHA-512:	D8C7FC594F24A631E1BADFDAFDB57BB6C431BC48B62998B5A226BDC7CE57A29061792A9F4E5DDC2389BE37AB1B507DA678FE4B31B34614F471BC2B802BB7E1B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108183157..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (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: 1000..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: 20210108183157..**********..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):	3.789835376583671

General

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:	2814976
MD5:	b87925c7eb04ed03b7d1b9a5a39358d8
SHA1:	cff199d7a3b2ecb1d5a6c2ba48de92901789cfda
SHA256:	8daa3b16b15dd52ffb99eb0644b52712d889fe9528f8633dd16b4b405b017130
SHA512:	0e9acf9fde99fc48dda2c878474d53716f4d574b2e488b4a80b96a9692f97a620efe9e14c7e1ab5c74c85808d2d38ef465cb489e210d0fe92dc1a3e6b35cf128
SSDEEP:	24576:H+x252KxvT7AGiQo6wvooXWR6p7fsqMPDTl2LRVa4IdO3Y9RpQ7aw7L9gLWg4cTg:uce6kaPDToi4IdWY67awV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.... "._.....d(.....(.. ....(...@.. .....`+....._)...@.....

File Icon

Icon Hash:	07d8d8d4d4d85026

Static PE Info

General

Entrypoint:	0x6882de
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:	0x5FF822B7 [Fri Jan 8 09:15:35 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x288284	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x28a000	0x28a50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x286800	0x1540	.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	
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	0x2862e4	0x286400	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x28a000	0x28a50	0x28c00	False	0.0466233703988	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	2.97289655472	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0x36c	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	IObit. All rights reserved.
FileVersion	13.0.0.49
CompanyName	IObit
LegalTrademarks	IObit
Comments	Advanced SystemCare Auto Sweep
ProductName	Advanced SystemCare
ProductVersion	13.0.0.49
FileDescription	Advanced SystemCare Auto Sweep
Guid	60b42ce5-df88-4b71-bf45-a33744fcf42a
Translation	0x0000 0x04e4

Possible Origin

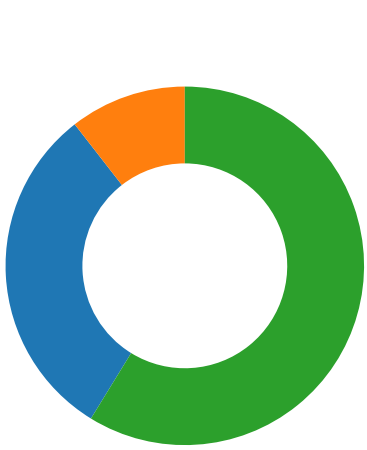
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 114

- 53 (DNS)
- 10004 undefined



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:31:24.376733065 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:31:24.416979074 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.417165041 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:31:24.461075068 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:31:24.501216888 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.504751921 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.504825115 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.504842997 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.504998922 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:31:24.511009932 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:31:24.551047087 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.551167011 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.591161966 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:31:24.618511915 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:31:24.658757925 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.666969061 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.667009115 CET	443	49710	104.23.99.190	192.168.2.5
Jan 8, 2021 18:31:24.667113066 CET	49710	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:18.068780899 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:18.109169960 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.109307051 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:18.348174095 CET	49731	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:18.350944996 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:18.391020060 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.393731117 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.393800020 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.393842936 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.393867970 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:18.397357941 CET	10004	49731	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:18.398782969 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:18.438940048 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.442034006 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.501873016 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:18.546454906 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:18.586724043 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.596575022 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.596632004 CET	443	49730	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:18.596720934 CET	49730	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:19.001941919 CET	49731	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:19.051101923 CET	10004	49731	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:19.689558983 CET	49731	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:19.739985943 CET	10004	49731	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:22.601443052 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:22.641594887 CET	443	49733	104.23.99.190	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:32:22.641721010 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:22.666995049 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:22.707395077 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.711358070 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.711397886 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.711416960 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.711523056 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:22.717020035 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:22.757294893 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.757844925 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.799159050 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:22.833534002 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:22.873955965 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.884177923 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.884222031 CET	443	49733	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:22.884385109 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:28.804842949 CET	49734	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:28.854245901 CET	10004	49734	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:29.502758980 CET	49734	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:29.551991940 CET	10004	49734	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:30.096587896 CET	49734	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:30.148751020 CET	10004	49734	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:36.389797926 CET	49735	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:36.439270973 CET	10004	49735	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:36.940993071 CET	49735	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:36.990786076 CET	10004	49735	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:37.503479958 CET	49735	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:37.553141117 CET	10004	49735	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:39.184977055 CET	49736	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:39.225265980 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.225397110 CET	49736	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:39.228811979 CET	49736	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:39.269016027 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.272711992 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.272732019 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.272748947 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.272902012 CET	49736	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:39.274951935 CET	49736	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:39.314965010 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.315071106 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.324415922 CET	49736	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:39.364463091 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.374560118 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.374582052 CET	443	49736	104.23.99.190	192.168.2.5
Jan 8, 2021 18:32:39.374672890 CET	49736	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:45.552649975 CET	49739	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:45.601923943 CET	10004	49739	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:46.048881054 CET	49733	443	192.168.2.5	104.23.99.190
Jan 8, 2021 18:32:46.191664934 CET	49739	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:46.240972042 CET	10004	49739	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:46.801114082 CET	49739	10004	192.168.2.5	194.5.97.173
Jan 8, 2021 18:32:46.850738049 CET	10004	49739	194.5.97.173	192.168.2.5
Jan 8, 2021 18:32:49.431197882 CET	49741	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:49.471458912 CET	443	49741	104.23.98.190	192.168.2.5
Jan 8, 2021 18:32:49.471576929 CET	49741	443	192.168.2.5	104.23.98.190
Jan 8, 2021 18:32:49.474611998 CET	49741	443	192.168.2.5	104.23.98.190

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:31:06.226120949 CET	54795	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:06.279073000 CET	53	54795	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:24.266156912 CET	49557	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:24.322529078 CET	53	49557	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:31:27.427134037 CET	61733	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:27.478928089 CET	53	61733	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:31.195940018 CET	65447	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:31.252470970 CET	53	65447	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:31.336635113 CET	52441	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:31.387371063 CET	53	52441	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:32.702754021 CET	62176	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:32.751205921 CET	53	62176	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:34.036644936 CET	59596	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:34.084470987 CET	53	59596	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:35.387299061 CET	65296	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:35.438033104 CET	53	65296	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:36.773515940 CET	63183	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:36.821496964 CET	53	63183	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:37.973342896 CET	60151	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:38.021277905 CET	53	60151	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:38.271847010 CET	56969	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:38.319643021 CET	53	56969	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:39.546310902 CET	55161	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:39.605269909 CET	53	55161	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:40.817363024 CET	54757	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:40.865215063 CET	53	54757	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:42.007613897 CET	49992	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:42.066764116 CET	53	49992	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:45.160653114 CET	60075	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:45.221355915 CET	53	60075	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:55.171797037 CET	55016	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:55.228377104 CET	53	55016	8.8.8.8	192.168.2.5
Jan 8, 2021 18:31:56.668503046 CET	64345	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:31:56.725179911 CET	53	64345	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:17.367624998 CET	57128	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:17.432390928 CET	53	57128	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:17.951802015 CET	54791	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:18.008084059 CET	53	54791	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:19.266114950 CET	50463	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:19.341434002 CET	53	50463	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:22.457204103 CET	50394	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:22.515639067 CET	53	50394	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:28.671607018 CET	58530	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:28.722496986 CET	53	58530	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:36.312988997 CET	53813	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:36.363810062 CET	53	53813	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:39.118150949 CET	63732	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:39.174691916 CET	53	63732	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:42.164417982 CET	57344	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:42.225449085 CET	53	57344	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:44.022420883 CET	54450	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:44.070389986 CET	53	54450	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:45.399282932 CET	59261	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:45.450463057 CET	53	59261	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:45.767371893 CET	57151	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:45.815238953 CET	53	57151	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:49.339917898 CET	59413	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:49.396167994 CET	53	59413	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:52.339349985 CET	60516	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:52.387439013 CET	53	60516	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:54.668682098 CET	51649	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:54.725019932 CET	53	51649	8.8.8.8	192.168.2.5
Jan 8, 2021 18:32:58.219737053 CET	65086	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:32:58.277734995 CET	53	65086	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:01.507724047 CET	56432	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:01.564433098 CET	53	56432	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:01.947154045 CET	52929	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:01.995008945 CET	53	52929	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:33:02.171906948 CET	64317	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:02.219821930 CET	53	64317	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:03.881963015 CET	61004	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:03.949186087 CET	53	61004	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:07.594350100 CET	56895	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:07.642417908 CET	53	56895	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:07.713891029 CET	62372	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:07.730717897 CET	61515	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:07.762573004 CET	53	62372	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:07.778650999 CET	53	61515	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:14.328829050 CET	56675	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:14.387923002 CET	53	56675	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:20.884196043 CET	57172	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:20.932195902 CET	53	57172	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:25.382311106 CET	55267	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:25.438584089 CET	53	55267	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:27.625704050 CET	50969	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:27.682338953 CET	53	50969	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:33.561655998 CET	64362	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:33.609699965 CET	53	64362	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:39.035249949 CET	54766	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:39.089112997 CET	53	54766	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:42.029217958 CET	61446	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:42.077615976 CET	53	61446	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:42.281184912 CET	57515	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:42.329241037 CET	53	57515	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:43.282241106 CET	58199	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:43.338522911 CET	53	58199	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:44.485451937 CET	65221	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:44.535326004 CET	53	65221	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:46.463371992 CET	61573	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:46.525743961 CET	53	61573	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:49.878412962 CET	56562	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:49.934824944 CET	53	56562	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:49.957849979 CET	53591	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:50.008671045 CET	53	53591	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:50.830368996 CET	59688	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:50.917220116 CET	53	59688	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:52.495915890 CET	56032	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:52.531183958 CET	61150	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:52.555049896 CET	53	56032	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:52.579680920 CET	53	61150	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:53.037260056 CET	63458	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:53.096657991 CET	53	63458	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:53.483895063 CET	50422	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:53.542552948 CET	53	50422	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:54.231245041 CET	53247	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:54.292819023 CET	53	53247	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:55.226639986 CET	58544	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:55.253365040 CET	53814	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:55.274454117 CET	53	58544	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:55.312272072 CET	53	53814	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:56.329108000 CET	51305	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:56.380157948 CET	53	51305	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:57.046292067 CET	53670	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:57.121478081 CET	53	53670	8.8.8.8	192.168.2.5
Jan 8, 2021 18:33:57.493902922 CET	55160	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:33:57.550358057 CET	53	55160	8.8.8.8	192.168.2.5
Jan 8, 2021 18:34:00.625790119 CET	61414	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:34:00.684886932 CET	53	61414	8.8.8.8	192.168.2.5
Jan 8, 2021 18:34:05.877055883 CET	63847	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:34:05.938656092 CET	53	63847	8.8.8.8	192.168.2.5
Jan 8, 2021 18:34:11.127619982 CET	61523	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:34:11.183722019 CET	53	61523	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:34:16.377371073 CET	50551	53	192.168.2.5	8.8.8.8
Jan 8, 2021 18:34:16.439781904 CET	53	50551	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 18:31:24.266156912 CET	192.168.2.5	8.8.8.8	0xb5d9	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:17.367624998 CET	192.168.2.5	8.8.8.8	0x9fbc	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:17.951802015 CET	192.168.2.5	8.8.8.8	0x9d37	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:22.457204103 CET	192.168.2.5	8.8.8.8	0xc0f5	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:28.671607018 CET	192.168.2.5	8.8.8.8	0x5b9d	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:36.312988997 CET	192.168.2.5	8.8.8.8	0x3f70	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:39.118150949 CET	192.168.2.5	8.8.8.8	0x6eb2	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:45.399282932 CET	192.168.2.5	8.8.8.8	0xc571	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:49.339917898 CET	192.168.2.5	8.8.8.8	0x4a4e	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:54.668682098 CET	192.168.2.5	8.8.8.8	0xef44	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:01.507724047 CET	192.168.2.5	8.8.8.8	0x9d5	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:07.594350100 CET	192.168.2.5	8.8.8.8	0xdc65	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:14.328829050 CET	192.168.2.5	8.8.8.8	0x9283	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:20.884196043 CET	192.168.2.5	8.8.8.8	0xa98e	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:25.382311106 CET	192.168.2.5	8.8.8.8	0x46f8	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:27.625704050 CET	192.168.2.5	8.8.8.8	0xb960	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:33.561655998 CET	192.168.2.5	8.8.8.8	0x69d5	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:39.035249949 CET	192.168.2.5	8.8.8.8	0xe8e	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:43.282241106 CET	192.168.2.5	8.8.8.8	0xcf54	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:44.485451937 CET	192.168.2.5	8.8.8.8	0x7d4	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:49.957849979 CET	192.168.2.5	8.8.8.8	0xbcc0	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:55.253365040 CET	192.168.2.5	8.8.8.8	0x43eb	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:00.625790119 CET	192.168.2.5	8.8.8.8	0x3792	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:05.877055883 CET	192.168.2.5	8.8.8.8	0xc60f	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:11.127619982 CET	192.168.2.5	8.8.8.8	0x2679	Standard query (0)	1.ispnano.dns-cloud.net	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:16.377371073 CET	192.168.2.5	8.8.8.8	0x194	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 18:31:24.322529078 CET	8.8.8.8	192.168.2.5	0xb5d9	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:31:24.322529078 CET	8.8.8.8	192.168.2.5	0xb5d9	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:17.432390928 CET	8.8.8.8	192.168.2.5	0x9fbc	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 18:32:18.008084059 CET	8.8.8.8	192.168.2.5	0x9d37	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:18.008084059 CET	8.8.8.8	192.168.2.5	0x9d37	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:22.515639067 CET	8.8.8.8	192.168.2.5	0xc0f5	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:22.515639067 CET	8.8.8.8	192.168.2.5	0xc0f5	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:28.722496986 CET	8.8.8.8	192.168.2.5	0x5b9d	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:36.363810062 CET	8.8.8.8	192.168.2.5	0x3f70	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:39.174691916 CET	8.8.8.8	192.168.2.5	0x6eb2	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:39.174691916 CET	8.8.8.8	192.168.2.5	0x6eb2	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:42.225449085 CET	8.8.8.8	192.168.2.5	0x137	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 8, 2021 18:32:45.450463057 CET	8.8.8.8	192.168.2.5	0xc571	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:49.396167994 CET	8.8.8.8	192.168.2.5	0x4a4e	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:49.396167994 CET	8.8.8.8	192.168.2.5	0x4a4e	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:32:54.725019932 CET	8.8.8.8	192.168.2.5	0xef44	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:01.564433098 CET	8.8.8.8	192.168.2.5	0x9d5	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:07.642417908 CET	8.8.8.8	192.168.2.5	0xdc65	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:14.387923002 CET	8.8.8.8	192.168.2.5	0x9283	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:20.932195902 CET	8.8.8.8	192.168.2.5	0xa98e	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:25.438584089 CET	8.8.8.8	192.168.2.5	0x46f8	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:25.438584089 CET	8.8.8.8	192.168.2.5	0x46f8	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:27.682338953 CET	8.8.8.8	192.168.2.5	0xb960	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:33.609699965 CET	8.8.8.8	192.168.2.5	0x69d5	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:39.089112997 CET	8.8.8.8	192.168.2.5	0xe8e	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:43.338522911 CET	8.8.8.8	192.168.2.5	0xcf54	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:43.338522911 CET	8.8.8.8	192.168.2.5	0xcf54	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:44.535326004 CET	8.8.8.8	192.168.2.5	0x7d4	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:33:50.008671045 CET	8.8.8.8	192.168.2.5	0xbcc0	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 18:33:55.312272072 CET	8.8.8.8	192.168.2.5	0x43eb	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:00.684886932 CET	8.8.8.8	192.168.2.5	0x3792	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:05.938656092 CET	8.8.8.8	192.168.2.5	0xc60f	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:11.183722019 CET	8.8.8.8	192.168.2.5	0x2679	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)
Jan 8, 2021 18:34:16.439781904 CET	8.8.8.8	192.168.2.5	0x194	No error (0)	1.ispnano.dns-cloud.net		194.5.97.173	A (IP address)	IN (0x0001)

HTTPS Packets

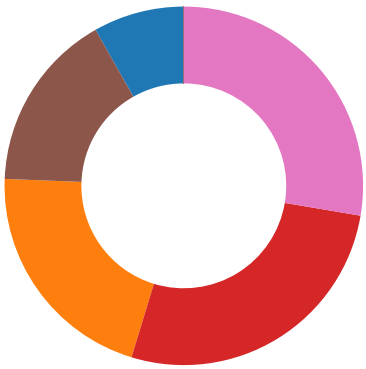
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 8, 2021 18:31:24.504842997 CET	104.23.99.190	443	192.168.2.5	49710	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc 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 18:32:18.393842936 CET	104.23.98.190	443	192.168.2.5	49730	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 18:32:22.711416960 CET	104.23.99.190	443	192.168.2.5	49733	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 18:32:39.272748947 CET	104.23.99.190	443	192.168.2.5	49736	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 18:32:49.520049095 CET	104.23.98.190	443	192.168.2.5	49741	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 18:33:26.442956924 CET	104.23.98.190	443	192.168.2.5	49759	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 18:33:43.452308893 CET	104.23.99.190	443	192.168.2.5	49765	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
- conhost.exe
- powershell.exe
- powershell.exe
- conhost.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- shipping order.exe
- cmd.exe
- conhost.exe
- timeout.exe
- cmd.exe
- conhost.exe
- shipping order.exe
- timeout.exe
- shipping order.exe
- shipping order.exe
- shipping order.exe

- WerFault.exe
- shipping order.exe
- powershell.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: shipping order.exe PID: 5316 Parent PID: 5708

General

Start time:	18:31:13
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:	0x7d0000
File size:	2814976 bytes
MD5 hash:	B87925C7EB04ED03B7D1B9A5A39358D8
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	6CACDD66	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	6CACDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\028a5345-3ada-4536-b4b8-e5892a029a73	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CACBEFF	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC7CF06	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	6DC7CF06	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 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 b7 22 f8 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 64 28 00 00 8e 02 00 00 00 00 00 de 82 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 91 5f 29 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...."._.......... ....d(...........(.. ....(...@.. ....` +......_)...@................	success or wait	6	6CACDD66	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	6CACDD66	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	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DC3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DC3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DC3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DC3D72F	unknown
C:\Users\user\Desktop\shipping order.exe	unknown	4096	success or wait	1	6DC3D72F	unknown
C:\Users\user\Desktop\shipping order.exe	unknown	512	success or wait	1	6DC3D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CAC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CAC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CAC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6CAC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6CAC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6CAC5F3C	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	6CAC646A	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	6CACC075	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	6CAC646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	shipping order.exe	unicode	C:\Users\user\Desktop\shipping order.exe	success or wait	1	6CAC646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\shipping order.exe	dword	0	success or wait	1	6CACC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6CACC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6CACC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6CACC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6CACC075	RegSetValueExW

Analysis Process: powershell.exe PID: 1000 Parent PID: 5316

General

Start time:	18:31:22
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:	0xfd0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CA25B28	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	6CA25B28	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC7CF06	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	6DC7CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_tiyw5ytt.diz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_jtqpnezb.p40.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	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	6CACBEFF	CreateDirectoryW
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.hrKQHeuP.20210108183125.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_tiyw5ytt.diz.ps1	success or wait	1	6CAC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_jtqpnezb.p40.psm1	success or wait	1	6CAC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_tiyw5ytt.diz.ps1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_jtqpnezb.p40.psm1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.hrKQHeuP.20210108183125.txt	unknown	3	ef bb bf	...	success or wait	1	6CAC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.hrKQHeuP.20210108183125.txt	unknown	737	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 33 31 35 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 61 6c 66 6f 6e 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 61 6c 66 6f 6e 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 35 37 39 35 36 39 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	********************..Windows PowerShell transcript start..Start time: 20210108183157..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6CAC1B4F	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 77 dc 65 ca 9f 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.....we....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	2	6CAC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 3c e1 65 ca 9f 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.....<.e....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	1	6CAC1B4F	WriteFile
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	1	6CAC1B4F	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	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	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	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	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	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	6DC6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	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	6CAC1B4F	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	6CAC1B4F	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	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	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	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	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	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	4	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile

Analysis Process: conhost.exe PID: 4668 Parent PID: 1000

General

Start time:	18:31:22
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 768 Parent PID: 5316

General

Start time:	18:31:22
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:	0xfd0000
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	6DC7CF06	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	6DC7CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ba2ypcd4.fal.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gz3jep32.ccp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.BT05d3d0.20210108183125.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ba2ypcd4.fal.ps1	success or wait	1	6CAC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gz3jep32.ccp.psm1	success or wait	1	6CAC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ba2ypcd4.fal.ps1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gz3jep32.ccp.psm1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.BT05d3d0.20210108183125.txt	unknown	3	ef bb bf	...	success or wait	1	6CAC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.BT05d3d0.20210108183125.txt	unknown	736	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 33 32 30 32 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 61 6c 66 6f 6e 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 61 6c 66 6f 6e 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 35 37 39 35 36 39 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	********************..Windows PowerShell transcript start..Start time: 20210108183202..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6CAC1B4F	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 77 dc 65 ca 9f 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.....we....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	2	6CAC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 3c e1 65 ca 9f 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.....<.e....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	1	6CAC1B4F	WriteFile
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	1	6CAC1B4F	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	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	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	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	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	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	6DC6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	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	6CAC1B4F	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	6CAC1B4F	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	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	126	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	69	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CAC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile

Analysis Process: conhost.exe PID: 5996 Parent PID: 768

General

Start time:	18:31:23
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 4724 Parent PID: 5316

General

Start time:	18:31:23
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:	0xfd0000
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

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	6DC7CF06	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	6DC7CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_sdzbntk1.vuf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_f13zkzre.whv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW
C:\Users\user\Documents\20210108\PowerShell_transcr ipt.579569.c+4r7aH8.20210108183126.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_sdzbntk1.vuf.ps1	success or wait	1	6CAC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_f13zkzre.whv.psm1	success or wait	1	6CAC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_sdzbntk1.vuf.ps1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_f13zkzre.whv.psm1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcr ipt.579569.c+4r7aH8.20210108183126.txt	unknown	3	ef bb bf	...	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcr ipt.579569.c+4r7aH8.20210108183126.txt	unknown	737	2a 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 33 32 30 35 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 61 6c 66 6f 6e 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 61 6c 66 6f 6e 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 35 37 39 35 36 39 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	**********..Windows PowerShell transcript start..Start time: 20210108183205..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6CAC1B4F	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 77 dc 65 ca 9f 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.....w.e....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	6CAC1B4F	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	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	6DC6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	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	6CAC1B4F	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	6CAC1B4F	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	6CAC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	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	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown

Analysis Process: powershell.exe PID: 4600 Parent PID: 5316

General

Start time:	18:31:23

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:	0xfd0000
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	6DC7CF06	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	6DC7CF06	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	6CA25B28	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	6CA25B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ydljvnmn.obz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dgie3wtq.dtl.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	CreateFileW
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.7jdhcRPS.20210108183127.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAC1E60	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	2	6CAC1E60	CreateFileW
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	5	6CA15C49	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	5	6CA15C49	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	6CA15C49	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CA15C49	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ydljvnmn.obz.ps1	success or wait	1	6CAC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dgie3wtq.dtl.psm1	success or wait	1	6CAC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ydljvnmn.obz.ps1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dgie3wtq.dtl.psm1	unknown	1	31	1	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.7jdhcRPS.20210108183127.txt	unknown	3	ef bb bf	...	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.579569.7jdhcRPS.20210108183127.txt	unknown	683	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 33 32 30 33 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 61 6c 66 6f 6e 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 61 6c 66 6f 6e 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 35 37 39 35 36 39 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	**********..Windows PowerShell transcript start..Start time: 20210108183203..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6CAC1B4F	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 77 dc 65 ca 9f 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.....w.e....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	2	6CAC1B4F	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 3c e1 65 ca 9f 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.....<.e.....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	1	6CAC1B4F	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	1	6CAC1B4F	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	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	6DC6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	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	6CAC1B4F	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	6CAC1B4F	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	6CAC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAC1B4F	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	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	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	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	70	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile

Analysis Process: conhost.exe PID: 5680 Parent PID: 4724

General

Start time:	18:31:23
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: conhost.exe PID: 5896 Parent PID: 4600

General

Start time:	18:31:23
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6292 Parent PID: 5316

General

Start time:	18:31:24
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:	0xd80000
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: 6320 Parent PID: 6292

General

Start time:	18:31:25
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6464 Parent PID: 6292

General

Start time:	18:31:25
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x3d0000
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: shipping order.exe PID: 6696 Parent PID: 3472

General

Start time:	18:31:32
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:	0x920000
File size:	2814976 bytes
MD5 hash:	B87925C7EB04ED03B7D1B9A5A39358D8
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: 0000000E.00000002.610896379.0000000004C82000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.610896379.0000000004C82000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.610896379.0000000004C82000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: cmd.exe PID: 6728 Parent PID: 5316

General

Start time:	18:31:32
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:	0xd80000
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: 6764 Parent PID: 6728

General

Start time:	18:31:33
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6820 Parent PID: 6728

General

Start time:	18:31:33
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x3d0000
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: cmd.exe PID: 1688 Parent PID: 5316

General

Start time:	18:31:39
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:	0xd80000
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: 4572 Parent PID: 1688

General

Start time:	18:31:39
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: shipping order.exe PID: 1624 Parent PID: 3472

General

Start time:	18:31:40
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:	0xa70000
File size:	2814976 bytes
MD5 hash:	B87925C7EB04ED03B7D1B9A5A39358D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: timeout.exe PID: 6460 Parent PID: 1688

General

Start time:	18:31:40
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x3d0000
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: 5860 Parent PID: 3472

General

Start time:	18:31:49
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:	0x6a0000
File size:	2814976 bytes

MD5 hash:	B87925C7EB04ED03B7D1B9A5A39358D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: shipping order.exe PID: 5732 Parent PID: 5316

General

Start time:	18:31:51
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:	0xbd0000
File size:	2814976 bytes
MD5 hash:	B87925C7EB04ED03B7D1B9A5A39358D8
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: 0000001E.00000002.551692234.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.551692234.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.551692234.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.606733051.00000000032E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.622773762.00000000042E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.622773762.00000000042E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: shipping order.exe PID: 6892 Parent PID: 3472

General

Start time:	18:31:58
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:	0x880000
File size:	2814976 bytes
MD5 hash:	B87925C7EB04ED03B7D1B9A5A39358D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: WerFault.exe PID: 5960 Parent PID: 5316

General

Start time:	18:31:59
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5316 -s 2616
Imagebase:	0xd00000
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: 6436 Parent PID: 3472

General

Start time:	18:32:07
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:	0xf10000
File size:	2814976 bytes
MD5 hash:	B87925C7EB04ED03B7D1B9A5A39358D8
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: 5128 Parent PID: 6696

General

Start time:	18:32:12
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:	0xfd0000
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: 5144 Parent PID: 5128

General

Start time:	18:32:13
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Disassembly

Code Analysis