ID: 346695
Sample Name: POinv00393.exe
Cookbook: default.jbs
Time: 13:28:16
Date: 01/02/2021
Version: 31.0.0 Emerald

Table of Contents

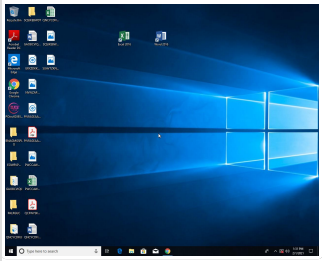
Analysis Report POinv00393.exe

Overview

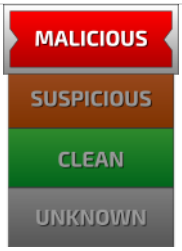
General Information

Sample Name:	POinv00393.exe
Analysis ID:	346695
MD5:	e0db9d12220a50..
SHA1:	b0af96f18727308..
SHA256:	09969e8d7af6e0c.
Tags:	exe HawkEye

Most interesting Screenshot:



Detection



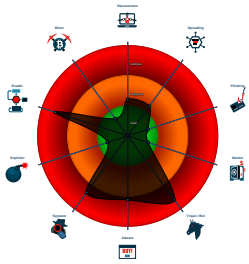
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Powershell adding …
- Yara detected AntiVM_3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- Adds a directory exclusion to Windo…
- Changes the view of files in windows…
- Connects to a pastebin service (like…
- Creates an undocumented autostart …

Classification



Startup

- **System is w10x64**
- POinv00393.exe (PID: 6708 cmdline: 'C:\Users\user\Desktop\POinv00393.exe' MD5: E0DB9D12220A5099BD1EBFEFC0CCDCFE)
  - powershell.exe (PID: 6892 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6916 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6980 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7080 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\POinv00393.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - POinv00393.exe (PID: 2100 cmdline: C:\Users\user\Desktop\POinv00393.exe MD5: E0DB9D12220A5099BD1EBFEFC0CCDCFE)
    - WerFault.exe (PID: 5556 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 1940 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- POinv00393.exe (PID: 6464 cmdline: 'C:\Users\user\Desktop\POinv00393.exe' MD5: E0DB9D12220A5099BD1EBFEFC0CCDCFE)
- POinv00393.exe (PID: 5436 cmdline: 'C:\Users\user\Desktop\POinv00393.exe' MD5: E0DB9D12220A5099BD1EBFEFC0CCDCFE)
- POinv00393.exe (PID: 2296 cmdline: 'C:\Users\user\Desktop\POinv00393.exe' MD5: E0DB9D12220A5099BD1EBFEFC0CCDCFE)
- POinv00393.exe (PID: 1784 cmdline: 'C:\Users\user\Desktop\POinv00393.exe' MD5: E0DB9D12220A5099BD1EBFEFC0CCDCFE)
- POinv00393.exe (PID: 5404 cmdline: 'C:\Users\user\Desktop\POinv00393.exe' MD5: E0DB9D12220A5099BD1EBFEFC0CCDCFE)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "mailpv",
    "WebBrowserPassView"
  ],
  "Version": ""
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000022.00000003.446565112.00000000051F0000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x12ce0:$key: HawkEyeKeylogger • 0x14f2c:$salt: 099u787978786 • 0x13347:$string1: HawkEye_Keylogger • 0x1419a:$string1: HawkEye_Keylogger • 0x14e8c:$string1: HawkEye_Keylogger • 0x13730:$string2: holdermail.txt • 0x13750:$string2: holdermail.txt • 0x13672:$string3: wallet.dat • 0x1368a:$string3: wallet.dat • 0x136a0:$string3: wallet.dat • 0x14a6e:$string4: Keylog Records • 0x14d86:$string4: Keylog Records • 0x14f84:$string5: do not script --> • 0x12cc8:$string6: \pidloc.txt • 0x12d3e:$string7: BSPLIT • 0x12d4e:$string7: BSPLIT
00000022.00000003.446565112.00000000051F0000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000022.00000003.446565112.00000000051F0000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x1339f:$hawkstr1: HawkEye Keylogger • 0x141e0:$hawkstr1: HawkEye Keylogger • 0x1450f:$hawkstr1: HawkEye Keylogger • 0x1466a:$hawkstr1: HawkEye Keylogger • 0x147cd:$hawkstr1: HawkEye Keylogger • 0x14a46:$hawkstr1: HawkEye Keylogger • 0x12f11:$hawkstr2: Dear HawkEye Customers! • 0x14562:$hawkstr2: Dear HawkEye Customers! • 0x146b9:$hawkstr2: Dear HawkEye Customers! • 0x14820:$hawkstr2: Dear HawkEye Customers! • 0x13032:$hawkstr3: HawkEye Logger Details:
00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7be38:$key: HawkEyeKeylogger • 0xfe258:$key: HawkEyeKeylogger • 0x180478:$key: HawkEyeKeylogger • 0x7e084:$salt: 099u787978786 • 0x1004a4:$salt: 099u787978786 • 0x1826c4:$salt: 099u787978786 • 0x7c49f:$string1: HawkEye_Keylogger • 0x7d2f2:$string1: HawkEye_Keylogger • 0x7dfe4:$string1: HawkEye_Keylogger • 0xfe8bf:$string1: HawkEye_Keylogger • 0xff712:$string1: HawkEye_Keylogger • 0x100404:$string1: HawkEye_Keylogger • 0x180adf:$string1: HawkEye_Keylogger • 0x181932:$string1: HawkEye_Keylogger • 0x182624:$string1: HawkEye_Keylogger • 0x7c888:$string2: holdermail.txt • 0x7c8a8:$string2: holdermail.txt • 0xfeca8:$string2: holdermail.txt • 0xfecc8:$string2: holdermail.txt • 0x180ec8:$string2: holdermail.txt • 0x180ee8:$string2: holdermail.txt
00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 8 entries				

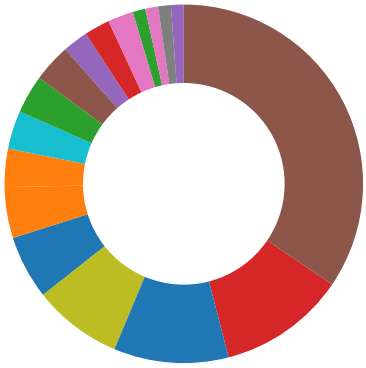
Sigma Overview

System Summary:

Sigma detected: Powershell adding suspicious path to exclusion list

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking



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

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses insecure TLS / SSL version for HTTPS connection
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected HawkEye Keylogger
- Installs a global keyboard hook

System Summary:

- Malicious sample detected (through community Yara rule)

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:

- Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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 HawkEye Keylogger

Yara detected MailPassView

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

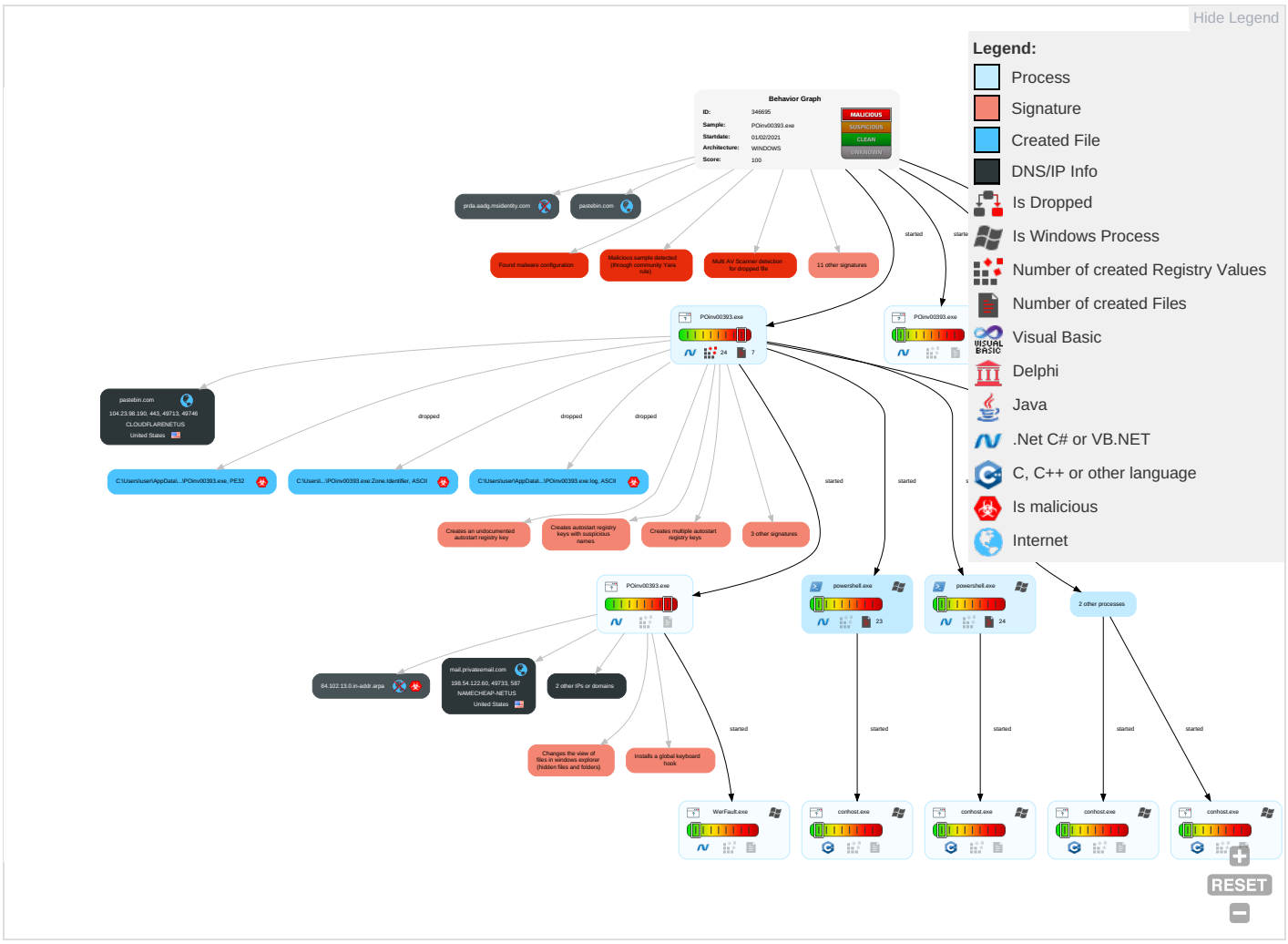
Detected HawkEye Rat

Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Replication Through Removable Media 1	Windows Management Instrumentation 2 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1 1	Input Capture 1 1	Peripheral Device Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 4 2 1	Process Injection 1 1 1	Obfuscated Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 4 2 1	Masquerading 1	Security Account Manager	System Information Discovery 1 3	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)	Virtualization/Sandbox Evasion 5	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 1	LSA Secrets	Security Software Discovery 1 4 1	SSH	Keylogging	Data Transfer Size Limits	Non-Applicatio Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applicatio Layer Protocol
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process 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	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

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
POinv00393.exe	34%	Virustotal		Browse
POinv00393.exe	18%	ReversingLabs	Win32.Trojan.Wacatac	
POinv00393.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe	18%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
84.102.13.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritaU	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.monotype.X	0%	Avira URL Cloud	safe	
http://www.fontbureau.comednxn	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnOx	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krW	0%	Avira URL Cloud	safe	
http://www.fontbureau.com(	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comueed	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	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://www.founder.com.c	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/sl-s	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krF4	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krK	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.sandoll.cQ	0%	Avira URL Cloud	safe	
http://en.wikip	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-nO	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/2	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comoitu:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF:	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/:	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krim	0%	Avira URL Cloud	safe	
http://www.fontbureau.comy	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.urwpp.del	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high
pastebin.com	104.23.98.190	true	false		high
84.102.13.0.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthrhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.fontbureau.coml.TTF	POinv00393.exe, 00000009.00000003.287512906.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddressxhttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comgritaU	POinv00393.exe, 00000009.00000003.332270630.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	POinv00393.exe, 00000009.00000003.269856466.00000000060A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

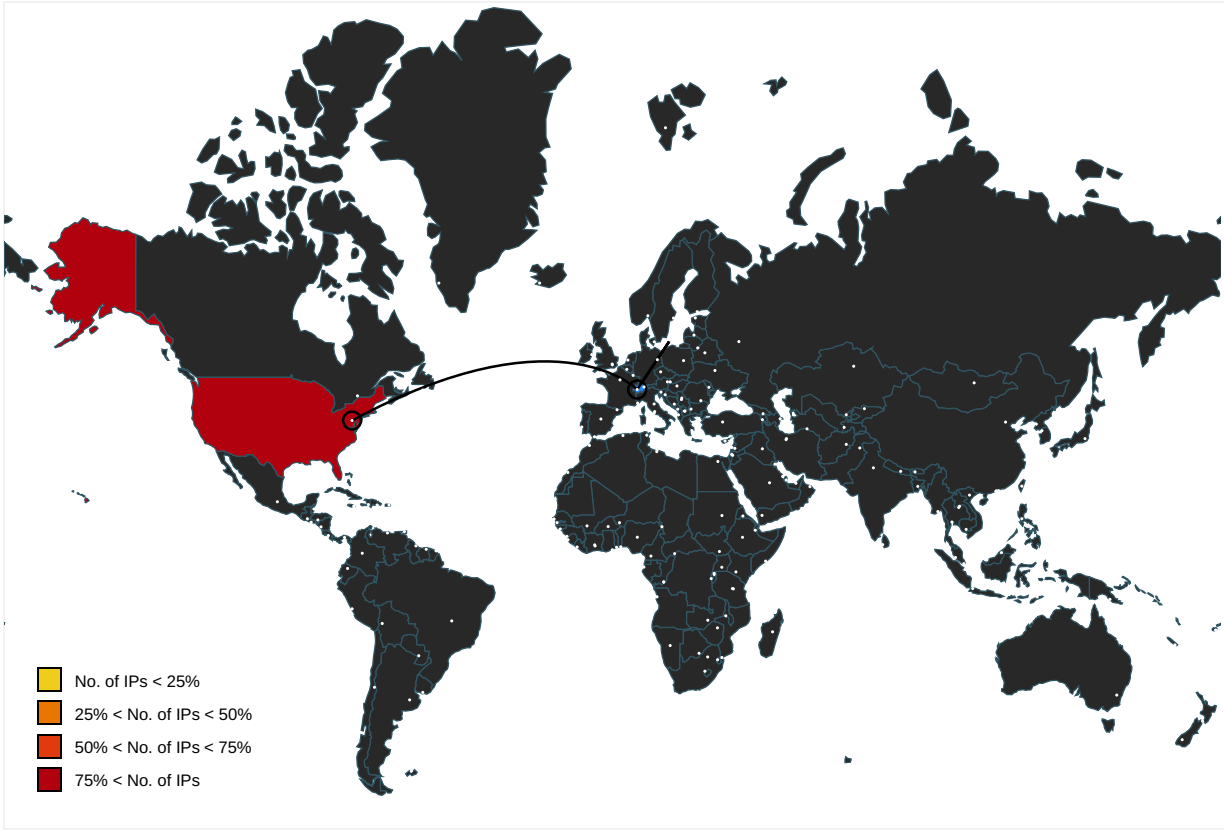
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	POinv00393.exe, 00000009.00000003.287512906.00000000060AA000.00000004.00000001.sdmp, POinv00393.exe, 00000009.00000003.292180727.00000000060AA000.00000004.00000001.sdmp, POinv00393.exe, 00000009.00000003.289173192.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comessed	POinv00393.exe, 00000009.00000003.295228473.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	POinv00393.exe, 00000009.00000003.262560956.00000000060AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	POinv00393.exe, 00000009.00000003.266388252.00000000060A8000.00000004.00000001.sdmp, POinv00393.exe, 00000009.00000003.266225699.00000000060A8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddressszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.monotype.X	POinv00393.exe, 00000009.00000003.300240186.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comednxn	POinv00393.exe, 00000009.00000003.289917470.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnOx	POinv00393.exe, 00000009.00000003.263686147.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krW	POinv00393.exe, 00000009.00000003.262560956.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com(	POinv00393.exe, 00000009.00000003.295228473.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://whatismyipaddress.com/-	POinv00393.exe, 00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp, WerFault.exe, 00000022.00000003.446565112.00000000051F0000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/	POinv00393.exe, 00000009.00000003.285625737.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	POinv00393.exe, 00000009.00000003.262220149.00000000060AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	POinv00393.exe, 00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp	false		high
http://www.urwpp.de	POinv00393.exe, 00000009.00000003.295228473.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	POinv00393.exe, 00000009.00000003.265749682.00000000060A7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000001.00000002.515543086.0000000004D91000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.575272180.0000000004541000.00000004.00000001.sdmp, WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	POinv00393.exe, 00000009.00000003.281094175.00000000060A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	POinv00393.exe, 00000009.00000003.285473287.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comueed	POinv00393.exe, 00000009.00000003.287512906.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerss	POinv00393.exe, 00000009.00000003.293691579.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersr	POinv00393.exe, 00000009.00000003.293691579.00000000060AA000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	POinv00393.exe, 00000009.00000003.332270630.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	POinv00393.exe, 00000009.00000003.304428786.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF	POinv00393.exe, 00000009.00000003.287512906.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/U	POinv00393.exe, 00000009.00000003.279036621.00000000060A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000001.00000002.522372632.0000000004ED2000.00000004.00000001.sdmp, powershell.exe, 00000005.00000003.416731741.00000000076A0000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.595455706.0000000004680000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000001.00000002.522372632.0000000004ED2000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.595455706.0000000004680000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000001.00000002.522372632.0000000004ED2000.00000004.00000001.sdmp, powershell.exe, 00000005.00000003.416731741.00000000076A0000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.595455706.0000000004680000.00000004.00000001.sdmp	false		high
http://www.founder.com.c	POinv00393.exe, 00000009.00000003.264142006.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/sl-s	POinv00393.exe, 00000009.00000003.279036621.00000000060A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.krF4	POinv00393.exe, 00000009.00000003.262560956.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krK	POinv00393.exe, 00000009.00000003.262560956.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comion	POinv00393.exe, 00000009.00000003.332270630.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wikipedia	POinv00393.exe, 00000009.00000003.261997834.00000000060AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.micr	powershell.exe, 00000003.00000002.598548034.0000000003377000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	POinv00393.exe, 00000009.00000003.279036621.00000000060A8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	POinv00393.exe, 00000009.00000003.295228473.00000000060AA000.00000004.00000001.sdmp, POinv00393.exe, 00000009.00000003.332270630.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.cQ	POinv00393.exe, 00000009.00000003.263201663.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.wikip	POinv00393.exe, 00000009.00000003.264750218.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	POinv00393.exe, 00000009.00000003.295228473.00000000060AA000.00000004.00000001.sdmp, POinv00393.exe, 00000009.00000003.289917470.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000001.00000002.522372632.0000000004ED2000.00000004.00000001.sdmp, powershell.exe, 00000002.00000003.416731741.00000000076A0000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.595455706.0000000004680000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnl-nO	POinv00393.exe, 00000009.00000003.263964185.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	POinv00393.exe, 00000009.00000003.266098249.00000000060A8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	POinv00393.exe, 00000009.00000003.264516630.00000000060A5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/y	POinv00393.exe, 00000009.00000003.279036621.00000000060A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	POinv00393.exe, 00000009.00000003.264396432.00000000060A5000.00000004.00000001.sdmp, POinv00393.exe, 00000009.00000003.263964185.00000000060AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	POinv00393.exe, 00000009.00000003.291895161.00000000060AA000.00000004.00000001.sdmp, POinv00393.exe, 00000009.00000003.289917470.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/2	POinv00393.exe, 00000009.00000003.301758986.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	POinv00393.exe, 00000009.00000003.291476719.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.monotype.	POinv00393.exe, 00000009.00000003.304428786.00000000060AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comoitu:	POinv00393.exe, 00000009.00000003.289917470.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000001.00000002.522372632.0000000004ED2000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.595455706.0000000004680000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	POinv00393.exe, 00000009.00000003.279036621.00000000060A8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTF:	POinv00393.exe, 00000009.00000003.295228473.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/:	POinv00393.exe, 00000009.00000003.301758986.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krim	POinv00393.exe, 00000009.00000003.262560956.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	POinv00393.exe, 00000009.00000003.287216804.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comy	POinv00393.exe, 00000009.00000003.285473287.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/h	POinv00393.exe, 00000009.00000003.276537694.00000000060A5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers=	POinv00393.exe, 00000009.00000003.286463158.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.urwpp.del	POinv00393.exe, 00000009.00000003.284582010.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprintrhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000022.00000003.438033658.0000000005620000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/o	POinv00393.exe, 00000009.00000003.285473287.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers0	POinv00393.exe, 00000009.00000003.285625737.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/	POinv00393.exe, 00000009.00000003.285473287.00000000060AA000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comnxa	POinv00393.exe, 00000009.00000003.266388252.00000000060A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comitud	POinv00393.exe, 00000009.00000003.295228473.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmWQ	POinv00393.exe, 00000009.00000003.314035977.00000000060AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.23.99.190	unknown	United States		13335	CLOUDFLARENETUS	false
104.23.98.190	unknown	United States		13335	CLOUDFLARENETUS	false
198.54.122.60	unknown	United States		22612	NAMECHEAP-NETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	346695
Start date:	01.02.2021
Start time:	13:28:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	POinv00393.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.spyw.evad.winEXE@30/27@7/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.42.151.234, 40.88.32.150, 104.43.139.144, 51.11.168.160, 92.122.144.200, 2.20.143.16, 2.20.142.210, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.104.144.132, 20.190.159.132, 40.126.31.6, 40.126.31.1, 40.126.31.137, 20.190.159.136, 40.126.31.141, 20.190.159.138, 40.126.31.135, 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, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.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, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, skypedataprdcolwus16.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 NtDeviceIoControlFile 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
13:29:17	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\POinv00393.exe
13:29:26	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run POinv00393.exe C:\Users\user\Desktop\POinv00393.exe
13:29:27	API Interceptor	21x Sleep call for process: POinv00393.exe modified
13:29:34	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\POinv00393.exe
13:29:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run POinv00393.exe C:\Users\user\Desktop\POinv00393.exe
13:29:51	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe
13:30:13	API Interceptor	208x Sleep call for process: powershell.exe modified

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
	1KITgJnGbI.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	DovV3LuJ6I.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
	I8r7e1pqac.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VrR9J0FnSG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	dEpoPWHmoI.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	zZp3oXclum.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	aTZQZVVriQ.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
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
	1KITgJnGbI.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
	aTZQZVVriQ.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pastebin.com	QuotationCVXpo00029392.exe	Get hash	malicious	Browse	• 104.23.98.190
	cbUJVTVJ.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.Trojan.Packed2.42783.20578.exe	Get hash	malicious	Browse	• 104.23.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INWARD-OUTWARD ANALYSIS.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	svchost.exe	Get hash	malicious	Browse	• 104.23.98.190
	0238-35-pdf.scr.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.tz.exe	Get hash	malicious	Browse	• 104.23.99.190
	fod1jZt8yK.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ for the supply of materialsservices for P.O. No. - 4700 001838.exe	Get hash	malicious	Browse	• 104.23.99.190
	Enq No 34 22-01-2021.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.mm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.Trojan.nm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.qm.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 104.23.98.190
	Design Specification_A2000006.doc	Get hash	malicious	Browse	• 104.23.99.190
mail.privateemail.com	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 198.54.122.60
	Pending Orders Statement -40064778.doc	Get hash	malicious	Browse	• 198.54.122.60
	documenting.doc	Get hash	malicious	Browse	• 198.54.122.60
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 198.54.122.60
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	Enq No 34 22-01-2021.exe	Get hash	malicious	Browse	• 198.54.122.60
	pickup receipt,DOC.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Trojan.nm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.qm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 198.54.122.60
	Pi_74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	New FedEx paper work review.exe	Get hash	malicious	Browse	• 198.54.122.60
	New paper work document attached.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL_AWB_1928493383.exe	Get hash	malicious	Browse	• 198.54.122.60
	PGXPHWCclJQdkUDcrlQETWlRbmXQw.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	MIR-CAR_MRC2021751030XMY,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	FACTURA.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	PO 642021.exe	Get hash	malicious	Browse	• 104.21.19.200
	00000000000000000090.exe	Get hash	malicious	Browse	• 172.67.188.154
	sample20210201-01.xlsm	Get hash	malicious	Browse	• 172.67.189.234
	NsNu725j8o.exe	Get hash	malicious	Browse	• 172.67.129.48
	FPZaxqP7uB.exe	Get hash	malicious	Browse	• 23.227.38.74
	AWB_SHIPPING_DOCUMENT_pdf.exe	Get hash	malicious	Browse	• 66.235.200.146
	DebitNote11_Owners Invoices.exe	Get hash	malicious	Browse	• 104.21.5.94
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 104.21.27.226
	New Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_1660392.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_1660392.doc	Get hash	malicious	Browse	• 172.67.188.154
	Bp93hBPMoi.exe	Get hash	malicious	Browse	• 104.21.86.207
	mEPx5H8svq.exe	Get hash	malicious	Browse	• 104.21.45.223
	HoFD3n7z6A.exe	Get hash	malicious	Browse	• 23.227.38.74
	BLWnF55j6W.exe	Get hash	malicious	Browse	• 104.21.45.223
	2Debit Note_OwnersInvoices.exe	Get hash	malicious	Browse	• 172.67.142.171
	20082020141903,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	PROFORMA INVOICE # ID40,pdf.exe	Get hash	malicious	Browse	• 162.159.135.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Swift MT 199_Pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	Inquiry.exe	Get hash	malicious	Browse	• 198.54.126.106
	AWB_SHIPPING_DOCUMENT_pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	imTmqTngvS.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL Details.exe	Get hash	malicious	Browse	• 198.54.114.191
	REMITTANCE ADVICE REF0000360261_PDF.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	Swift copy.xls	Get hash	malicious	Browse	• 199.188.200.124
	Orders.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL Details.exe	Get hash	malicious	Browse	• 198.54.126.165
	order.doc	Get hash	malicious	Browse	• 199.188.201.34
	aOn5CfTiwS.exe	Get hash	malicious	Browse	• 198.54.117.244
	PO_55004.exe	Get hash	malicious	Browse	• 68.65.122.156
	SecuriteInfo.com.Trojan.MulDrop16.10041.23448.exe	Get hash	malicious	Browse	• 185.61.153.111
	SecuriteInfo.com.Trojan.Inject4.6821.6799.exe	Get hash	malicious	Browse	• 199.188.200.150
	DCAjXz5y4I.exe	Get hash	malicious	Browse	• 162.213.255.196
	NEW ORDER.xlsm	Get hash	malicious	Browse	• 104.219.248.89
	Claim_250196008_01282021.xls	Get hash	malicious	Browse	• 162.0.226.110
	Claim_250196008_01282021.xls	Get hash	malicious	Browse	• 162.0.226.110
	lbqFKoALqe.exe	Get hash	malicious	Browse	• 198.54.117.215
CLOUDFLARENETUS	MIR-CAR_MRC2021751030XMY,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	FACTURA.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	PO 642021.exe	Get hash	malicious	Browse	• 104.21.19.200
	00000000000000000090.exe	Get hash	malicious	Browse	• 172.67.188.154
	sample20210201-01.xlsm	Get hash	malicious	Browse	• 172.67.189.234
	NsNu725j8o.exe	Get hash	malicious	Browse	• 172.67.129.48
	FPZaxqP7uB.exe	Get hash	malicious	Browse	• 23.227.38.74
	AWB_SHIPPING_DOCUMENT_pdf.exe	Get hash	malicious	Browse	• 66.235.200.146
	DebitNote11_Owners Invoices.exe	Get hash	malicious	Browse	• 104.21.5.94
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 104.21.27.226
	New Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_1660392.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_1660392.doc	Get hash	malicious	Browse	• 172.67.188.154
	Bp93hBPMoi.exe	Get hash	malicious	Browse	• 104.21.86.207
	mEPx5H8svq.exe	Get hash	malicious	Browse	• 104.21.45.223
	HoFD3n7z6A.exe	Get hash	malicious	Browse	• 23.227.38.74
	BLWnF55j6W.exe	Get hash	malicious	Browse	• 104.21.45.223
	2Debit Note_OwnersInvoices.exe	Get hash	malicious	Browse	• 172.67.142.171
	20082020141903,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	PROFORMA INVOICE # ID40,pdf.exe	Get hash	malicious	Browse	• 162.159.135.233

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	PO 642021.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	00000000000000000090.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	New Order.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	IMG_1660392.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	mEPx5H8svq.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	NS_PO_86655443.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	INV#1191189.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	NEW PURCHASE#U00c3#U00bf #U00c3#U00bfORDER.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	CITI SOLUTION COMPANY PROFILE.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QuotationCVXpo00029392.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Orders.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	DOCUMENT.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Hydro-463459.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	Payment Document.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	CHIKWA (2).exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	gGQWGJWR4jzvzse.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	cbUJVTVJ.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	SecuriteInfo.com.Trojan.Packed2.42783.20578.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	file.exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190
	PURCHASE ORDER..exe	Get hash	malicious	Browse	• 104.23.98.190 • 104.23.99.190

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF9.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 1 21:30:59 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	537274
Entropy (8bit):	3.9310595429624575
Encrypted:	false
SSDEEP:	3072:L++noJgF6OH6CvXiyek0sjd+ptBiDNuk0rbA9gIOgF5iRRgsb0OPvyJSUCgUrwZ9:L+iLUvCvlV0dpbDrbA9RpD6bNTjk1N
MD5:	4170235DECFA153A91261EE362565641
SHA1:	C4F7ABBF1F75FA08B540E2C09A3DC6447CE53518
SHA-256:	C4061794E5D6A7C38311A28EE04AB4707AEAB633E5DF323F968E884BB608E9B3
SHA-512:	88722DAD35F603F6BAB9BEC992262A94F2021FA3F5327FAB2638AB155D4F85A18ECA5772F26CC74C74E4729CAACECFAD91EE6ABF2E63AA4FAAE024D298201A78
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....s.`.....U.....B.....V.....GenuineIntelW.....T.....4....r.`.....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:\ProgramData\Microsoft\Windows\WER\Temp\WERBC13.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):	8360
Entropy (8bit):	3.690213391871293
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFjp6x06Yrm6OgmfZeex8S4CprX89bgksf0amAm:RrlsNi5p6C6YK6OgmffWSIgXfXI
MD5:	80D4AD7A73773992C856046E6E725643
SHA1:	34C802EE7CCAB28F42FCC49B7A53CF1D6F93B370
SHA-256:	8357FAE75D84A0AD351DCB4F4D995F15DB75066FD25E637CBD0CEF03997ABE63
SHA-512:	AB0925156DB78C8275AE77EB57AC1ACAABB20E85C051F7578915C18F60ED9258383C07E7E3AECE77623C58EBD75B998D0624FEDB189F917474057BA67E302CF1
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBC13.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.1.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC7D.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4732
Entropy (8bit):	4.463218689409153
Encrypted:	false
SSDEEP:	48:cvIwSD8zspNJgtWI9cqWSC8Bhs8fm8M4JwquFB+q8v2/JhDg+oIrd:uITfJzLSN7RJwnKuJhDg+xrd
MD5:	3DAC03AA4D4A5D77A84C1C14B8B998CB
SHA1:	1E66988AAD28CCAF1995F35C7BFECE34FB604467
SHA-256:	D559D3756FCDBB5F2D9D0D66674D21DC27AFD5C4BEDDA0BD785DAEB464C30C7E
SHA-512:	FD75BFAE58A93889EB78FE1AF54DD69E4857A28731D1AB834FA3EB27851F906A2468BCCA8DA470F9BD42D5536E9A70CA1B1ADAC6473CF90815240599CBC8BE05
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="842801" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POinv00393.exe.log	
Process:	C:\Users\user\Desktop\POinv00393.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:MLU84qpE4Ks2wKDE4KhK3VZ9pKhIE4KnKIE4oKFKHKoZAE4Kzr7a:Mgv2HKXwYHKhQnoIHKntHoxHhAHKzva
MD5:	2AAAF19599DBB7B2B9269F77209C4FBA
SHA1:	17286C6FB357C72FFC81EE46EF05575A1AE134FD
SHA-256:	5B8D713F6F10790AF314D4AD256EB7A6BB156912034148D50955AF724FD0F2A4
SHA-512:	8C2E41464E18768F1ABA2CEC8DBBC8C234F538AB01F381ECCF22F865E2624EEFC362E6099C94C1603359FB42C55D2E8F142E44A7DA2B746DFE858811BDFDEEBF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

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):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	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.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	20608
Entropy (8bit):	5.577957281049141
Encrypted:	false
SSDEEP:	384:2t9D+w+8aWA0kzKJwSBKniuItIo3D7Y9gxSJUeRe1qMymF+ZSRx1ldM:yjA+w4Kiultp33xXe+N+9
MD5:	19620665888D6D08F76E36D7436A40C8
SHA1:	04DC1F73E61645D46EA229427E62BADF8DD1D42C
SHA-256:	9CD284466BA35D94F39FFCB8513B387F24F8B3A4F23B46FEBC2600D0985878B8
SHA-512:	D281644896FDDC7BDCF0E602B1FAC36CB4E7BC9107C1E3AB5017F071F743C3689BF4BAE452D9456A8F24160AFF97B28BFA07AA2F00AA5892EF5D518D5AE126 4
Malicious:	false
Preview:	@...e.....R.B.....<.....@.....H.....<@.^.L."My...:<..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)q.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1jbb1rur.kxs.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_3gd4shtk.lf5.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_ap14tuqv.fkf.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ap14tuqv.fkf.ps1	
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_btp5zmxs.mrt.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_igqs5mg1.0fv.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_ita4axrx.vfc.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_q0eyjx0q.um5.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q0eyjx0q.um5.psm1	
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_rrwl3rrp.fl5.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe	
Process:	C:\Users\user\Desktop\POinv00393.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4552704
Entropy (8bit):	2.8112977525077643
Encrypted:	false
SSDEEP:	6144:45eP+kQFHJWrhOJUFCfAYes4yP5GgU6NbimHWMJ97/1W3lTYSKVSIrSFoiGPciaW:45eP+kOnEC
MD5:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
SHA1:	B0AF96F187273082687F2C58FACA71B837876429
SHA-256:	09969E8D7AF6E0C3EF34C344FE378DD23B6F93ABCDA793C052E36D1777C35CE7
SHA-512:	297E6B7A0A22BDD42572C761894826131EB18986A8D0CCD0F092FF21249FA38F1911CBEB14E29571843F2A3D5C0FEBE50D1859757B35A52F952D54521BC2A286
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 18%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...sU.`.....".."...P...C.....C.. ....D...@.. ..... E.....@.....`.C.K.....D. .....E..... ....H.....text.....C.. ....C..... ..`.rsrc... .....D.....C..... ..@..@.reloc.....E.....vE.....@..B.....C.....H.....8....C.....$.....**....(....*~~g...:....(2...s.....g...~g...*. ....*.....90...((...9.....r.FCp....(.. ..(....*.....(....*....*2rtGCp.()...*2r.GCp.()...*2r.GCp.()...*2r.HCp.()...*.....(....*..0.....(#...("...(!...(...(....(....(....(....(....(....(.....d...(....(....(.....c...(....(....(.....b...(....(.... (.....a...(....(....(.....`...(....(....(....._...(....(....(.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\POinv00393.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\POinv00393.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:E:E
MD5:	2CAD8FA47BBEF282BADBB8DE5374B894
SHA1:	89B98F7BE8AFC23EBEFC3E02F86EBB89CBE74176
SHA-256:	4F5131EA0C5A3E7F4C5F86029AE1BE2A60E67F023073BBB074A3A929089E5BC1
SHA-512:	149D27069D40BCB60EA6A635B8E34E8B31FAD19D388C36B3FC8D6DF21F84D4A8DBC8BD05B127102960C9060771C76A8CC836F14B23D1EEA2B0D6CFA5C2B0B BB
Malicious:	false
Preview:	 2100

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\POinv00393.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.486348298002912
Encrypted:	false
SSDEEP:	3:oNWXp5v1qKrWcBC:oNWXpFgKrY
MD5:	41637FB0193F907F1ABEB6F39EEA4577
SHA1:	4CEED84E860A6DE18CBD6E9DF4FE86B698B25D0B
SHA-256:	FDB0215F49C0EE51BC759CDA39669B5220FCF7591B3F22A22B06E372697B4B2F
SHA-512:	0B7627D614BF73329BF223A9DD2692241E63D8707377DF86F4CD7D244C4E872BE4E2FA417D5DE939325E7F95B9D4DA6FD6AD4B7BC22A7D8E06AF3A56BD0B4C B
Malicious:	false
Preview:	 C:\Users\user\Desktop\POinv00393.exe

C:\Users\user\Documents\20210201\PowerShell_transcript.878164.GqBDotby.20210201132918.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):	3809
Entropy (8bit):	5.339806385613069
Encrypted:	false
SSDEEP:	96:BZ+haNn2qDo1ZpO1ZIhaNn2qDo1ZmqTp0cp0cp07TZpq:Mlly/q
MD5:	5A3DCAAE0A180D627E433BF5B402255C
SHA1:	C32CA03F2A01A4865B4A4140EA32A019152B3079
SHA-256:	CBA172347D512F02BD657F1FA1861B7DA7F0221D23D9614195ADC9A7674FD386
SHA-512:	BBC8450AAA16B0A3D3BE97845A8B6AA1664970FA9369BAEA9146A8FCD47A4ACB925E69DAC1C363D4C7CA0A6F7D19E62C4503DBDFA0D32BA5840ED13DA206E AF7
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210201132952..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878164 (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\POinv00393.exe -Force..Process ID: 6980..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: 20210201132953..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe -Force..**********..Command start time: 2021

C:\Users\user\Documents\20210201\PowerShell_transcript.878164.RDa_5qiQ.20210201132920.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):	5127
Entropy (8bit):	5.417997189198616
Encrypted:	false
SSDEEP:	96:BZchaNkqDo1ZqZphaNkqDo1ZZqUSjZ+haNkqDo1Zs3C9:3
MD5:	6F5B038D676CABE9FE4AF2C24545A590
SHA1:	02B83A0FB6706B92BF51AACAECA5C00BC7DD7490
SHA-256:	DDED7AD2F51FCCF981F5BFDC8312247CC671FF02A871EC733870F3FDE4C1F6E1

C:\Users\user\Documents\20210201\PowerShell_transcript.878164.RDa_5qiQ.20210201132920.txt	
SHA-512:	7D37E4B98E05AB946FD7F3AE82D4FB232F49C64265F80FFD33EE156BCDE68FF7A7DE85814A2C0780C3106690D6E9F0D41C29FF2B3F15C012A21ECA83CD6B990
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210201132954..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878164 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\POinv00393.exe -Force..Process ID: 7080..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: 20210201132955..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\POinv00393.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210201133945..Username: computer\user..RunAs User: computer\user.

C:\Users\user\Documents\20210201\PowerShell_transcript.878164.RU3nUHy1.20210201132916.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):	3809
Entropy (8bit):	5.340275685599787
Encrypted:	false
SSDEEP:	96:BZOhaNneqDo1ZvZ1ZehaNneqDo1Z8qTp0cp0cp02ZF:Nll9
MD5:	714E2032E0E9D32A72BEBE0E8CCBF0BD
SHA1:	0A99BF1E3D745DE47BAD3AA441075A7EE13D1685
SHA-256:	7FC0B1528ED7ACB4E1D1228FCE35B417158D06057B4CC521314674BE59AF5DD0
SHA-512:	C74A391C87C9D4003F3EFC503166746986066B1AF09CB2938DA60A3C09AEBB552E0796DA53764169BF6CE889145F61C37B0BF1699E6F705FE00E3E35EA7B07A8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210201132945..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878164 (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\POinv00393.exe -Force..Process ID: 6892..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: 20210201132946..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe -Force..**********..Command start time: 2021

C:\Users\user\Documents\20210201\PowerShell_transcript.878164.c22VO1SZ.20210201132917.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):	3809
Entropy (8bit):	5.339367409959746
Encrypted:	false
SSDEEP:	96:BZ/haNnzqDo1ZpO1ZjhaNnzqDo1ZXqTp0cp0cp04ZI:NllC
MD5:	A803ABA6CCBBBD437B5FEDB28EF7551E
SHA1:	1A2EF0D582DC12737036765A9CFF386F8C718891
SHA-256:	B24F498A88C1404D59DF3CD42346D6DF6FF809F970E8A4EC0813F104000E1F14
SHA-512:	77B79CE756D75E5B725F191198736AAE3D6854177286C634E33BEC483E8EF2C3305499716F8C431FCB34C55319B3591FDF95300FE544144D086467C283737F33
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210201132953..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878164 (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\POinv00393.exe -Force..Process ID: 6916..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: 20210201132953..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe -Force..**********..Command start time: 2021

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.8112977525077643
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%

General

File name:	POinv00393.exe
File size:	4552704
MD5:	e0db9d12220a5099bd1ebfefc0ccdcfe
SHA1:	b0af96f187273082687f2c58faca71b837876429
SHA256:	09969e8d7af6e0c3ef34c344fe378dd23b6f93abcda793c052e36d1777c35ce7
SHA512:	297e6b7a0a22bdd42572c761894826131eb18986a8d0cc d0f092ff21249fa38f1911cbeb14e29571843f2a3d5c0febe 50d1859757b35a52f952d54521bc2a286
SSDEEP:	6144:45eP+kQFHJWrhOJUFCfAYes4yP5GgU6NbimH WMJ97/1W3lTYSKVSIrSFoiGPciaW:45eP+kOnEC
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L...s U.`.....".."...P...C.....C.. ....D...@.. .....E... .....@.....

File Icon

Icon Hash:	1731ec421a143187

Static PE Info

General

Entrypoint:	0x83fbae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60175573 [Mon Feb 1 01:12:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x43fb60	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x440000	0x19720	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x45a000	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	0x43dbb4	0x43dc00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x440000	0x19720	0x19800	False	0.400821461397	data	4.61510693339	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x45a000	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	0x4401f0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x440658	0x10a8	data		
RT_ICON	0x441700	0x25a8	data		
RT_ICON	0x443ca8	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	0x447ed0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 33554431, next used block 33554431		
RT_GROUP_ICON	0x4586f8	0x4c	data		
RT_VERSION	0x458744	0x324	data		
RT_MANIFEST	0x458a68	0xcb8	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

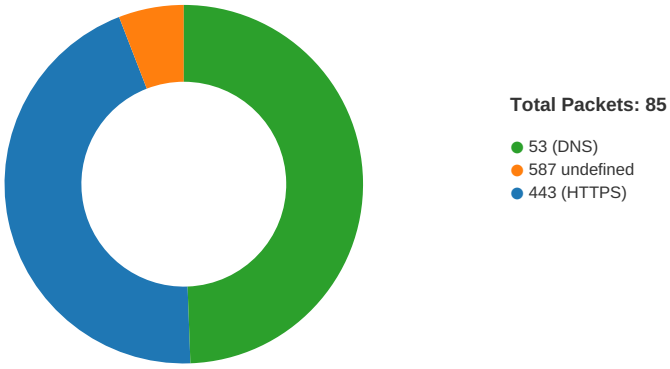
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	RunFirst.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	WindowsApp4
ProductVersion	1.0.0.0
FileDescription	WindowsApp4
OriginalFilename	RunFirst.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 13:29:16.513447046 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:16.553508997 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.553692102 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:16.601013899 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:16.641140938 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.645549059 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.645612955 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.645644903 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.645734072 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:16.650084972 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:16.690104961 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.690501928 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.732094049 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:16.771965027 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:16.814507008 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.861993074 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.862031937 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.862070084 CET	443	49713	104.23.98.190	192.168.2.3
Feb 1, 2021 13:29:16.862097025 CET	49713	443	192.168.2.3	104.23.98.190

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 13:29:16.903844118 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:29:27.112786055 CET	49713	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:30:24.753370047 CET	49733	587	192.168.2.3	198.54.122.60
Feb 1, 2021 13:30:24.947505951 CET	587	49733	198.54.122.60	192.168.2.3
Feb 1, 2021 13:30:24.947632074 CET	49733	587	192.168.2.3	198.54.122.60
Feb 1, 2021 13:30:25.142040968 CET	587	49733	198.54.122.60	192.168.2.3
Feb 1, 2021 13:30:25.150007010 CET	49733	587	192.168.2.3	198.54.122.60
Feb 1, 2021 13:30:25.345731974 CET	587	49733	198.54.122.60	192.168.2.3
Feb 1, 2021 13:30:25.345933914 CET	587	49733	198.54.122.60	192.168.2.3
Feb 1, 2021 13:30:25.387917042 CET	49733	587	192.168.2.3	198.54.122.60
Feb 1, 2021 13:30:25.581036091 CET	587	49733	198.54.122.60	192.168.2.3
Feb 1, 2021 13:30:25.626442909 CET	49733	587	192.168.2.3	198.54.122.60
Feb 1, 2021 13:30:35.580713034 CET	587	49733	198.54.122.60	192.168.2.3
Feb 1, 2021 13:31:18.384181976 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:18.424554110 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.424674034 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:18.659849882 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:18.699973106 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.708345890 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.708395958 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.708425999 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.708525896 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:18.712896109 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:18.752990961 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.757481098 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.844849110 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:18.886878014 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.906265974 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.906311989 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.906337976 CET	443	49742	104.23.99.190	192.168.2.3
Feb 1, 2021 13:31:18.906949043 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:29.612466097 CET	49742	443	192.168.2.3	104.23.99.190
Feb 1, 2021 13:31:42.450350046 CET	49746	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:42.490411043 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.491337061 CET	49746	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:42.494322062 CET	49746	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:42.534347057 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.537802935 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.537851095 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.537899971 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.537921906 CET	49746	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:42.539942026 CET	49746	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:42.580662966 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.581034899 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.587011099 CET	49746	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:42.627904892 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.646184921 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.646214008 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.646239996 CET	443	49746	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:42.646367073 CET	49746	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.166985035 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.207155943 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.207385063 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.237140894 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.277282000 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.280203104 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.280266047 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.280311108 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.280325890 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.289315939 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.331962109 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.332104921 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.344928980 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.386651993 CET	49749	443	192.168.2.3	104.23.98.190

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 13:31:44.387746096 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.413476944 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.413510084 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.413537979 CET	443	49748	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.413568020 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.426853895 CET	443	49749	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.427016973 CET	49749	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.444993019 CET	49749	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.461222887 CET	49748	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.485136986 CET	443	49749	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.487859964 CET	443	49749	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.487879038 CET	443	49749	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.487889051 CET	443	49749	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.488208055 CET	49749	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.489525080 CET	49749	443	192.168.2.3	104.23.98.190
Feb 1, 2021 13:31:44.529505968 CET	443	49749	104.23.98.190	192.168.2.3
Feb 1, 2021 13:31:44.531852961 CET	443	49749	104.23.98.190	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 13:28:59.216948032 CET	64185	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:28:59.264928102 CET	53	64185	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:00.127966881 CET	65110	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:00.176038027 CET	53	65110	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:01.269016027 CET	58361	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:01.317019939 CET	53	58361	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:02.516761065 CET	63492	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:02.569441080 CET	53	63492	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:13.349462032 CET	60831	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:13.397661924 CET	53	60831	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:16.431164026 CET	60100	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:16.490526915 CET	53	60100	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:20.900108099 CET	53195	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:20.948139906 CET	53	53195	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:23.858836889 CET	50141	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:23.911160946 CET	53	50141	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:24.810740948 CET	53023	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:24.860874891 CET	53	53023	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:25.646713018 CET	49563	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:25.696690083 CET	53	49563	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:26.833936930 CET	51352	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:26.882045984 CET	53	51352	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:28.218255997 CET	59349	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:28.279561996 CET	53	59349	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:29.304369926 CET	57084	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:29.352374077 CET	53	57084	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:31.726248980 CET	58823	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:31.777128935 CET	53	58823	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:32.818933010 CET	57568	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:32.866981030 CET	53	57568	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:33.843837976 CET	50540	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:33.904483080 CET	53	50540	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:38.807836056 CET	54366	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:38.857064009 CET	53	54366	8.8.8.8	192.168.2.3
Feb 1, 2021 13:29:49.351733923 CET	53034	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:29:49.418762922 CET	53	53034	8.8.8.8	192.168.2.3
Feb 1, 2021 13:30:02.960099936 CET	57762	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:30:03.017563105 CET	53	57762	8.8.8.8	192.168.2.3
Feb 1, 2021 13:30:13.738193035 CET	55435	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:30:13.804760933 CET	53	55435	8.8.8.8	192.168.2.3
Feb 1, 2021 13:30:16.272480011 CET	50713	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:30:16.331005096 CET	53	50713	8.8.8.8	192.168.2.3
Feb 1, 2021 13:30:24.550024986 CET	56132	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 13:30:24.606308937 CET	53	56132	8.8.8.8	192.168.2.3
Feb 1, 2021 13:30:47.385190964 CET	58987	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:30:47.437189102 CET	53	58987	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:01.019228935 CET	56579	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:01.077106953 CET	53	56579	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:18.281862020 CET	60633	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:18.341321945 CET	53	60633	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:22.709028959 CET	61292	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:22.758601904 CET	53	61292	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:23.435662031 CET	63619	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:23.507647991 CET	53	63619	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:42.382093906 CET	64938	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:42.429873943 CET	53	64938	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:42.933465958 CET	61946	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:42.992605925 CET	53	61946	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:44.069084883 CET	64910	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:44.120579958 CET	53	64910	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:44.161408901 CET	52123	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:44.220738888 CET	53	52123	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:44.798934937 CET	56130	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:44.858637094 CET	53	56130	8.8.8.8	192.168.2.3
Feb 1, 2021 13:31:59.554116011 CET	56338	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:31:59.614866018 CET	53	56338	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:01.269294977 CET	59420	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:01.326045990 CET	53	59420	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:02.431868076 CET	58784	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:02.490565062 CET	53	58784	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:05.613373041 CET	63978	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:05.675867081 CET	53	63978	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:06.200283051 CET	62938	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:06.256623983 CET	53	62938	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:06.672820091 CET	55708	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:06.732122898 CET	53	55708	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:07.253746986 CET	56803	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:07.311764002 CET	53	56803	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:07.870692015 CET	57145	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:07.930886030 CET	53	57145	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:08.562553883 CET	55359	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:08.613559008 CET	53	55359	8.8.8.8	192.168.2.3
Feb 1, 2021 13:32:09.056766033 CET	58306	53	192.168.2.3	8.8.8.8
Feb 1, 2021 13:32:09.114964008 CET	53	58306	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 1, 2021 13:29:16.431164026 CET	192.168.2.3	8.8.8.8	0x3d6d	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Feb 1, 2021 13:30:16.272480011 CET	192.168.2.3	8.8.8.8	0x39c2	Standard query (0)	84.102.13.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 1, 2021 13:30:24.550024986 CET	192.168.2.3	8.8.8.8	0x5160	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:18.281862020 CET	192.168.2.3	8.8.8.8	0xc79a	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:42.382093906 CET	192.168.2.3	8.8.8.8	0x473e	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:44.069084883 CET	192.168.2.3	8.8.8.8	0xb976	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:44.161408901 CET	192.168.2.3	8.8.8.8	0x75b8	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 1, 2021 13:29:16.490526915 CET	8.8.8.8	192.168.2.3	0x3d6d	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 1, 2021 13:29:16.490526915 CET	8.8.8.8	192.168.2.3	0x3d6d	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:30:16.331005096 CET	8.8.8.8	192.168.2.3	0x39c2	Name error (3)	84.102.13.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 1, 2021 13:30:24.606308937 CET	8.8.8.8	192.168.2.3	0x5160	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:18.341321945 CET	8.8.8.8	192.168.2.3	0xc79a	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:18.341321945 CET	8.8.8.8	192.168.2.3	0xc79a	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:42.429873943 CET	8.8.8.8	192.168.2.3	0x473e	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:42.429873943 CET	8.8.8.8	192.168.2.3	0x473e	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:42.992605925 CET	8.8.8.8	192.168.2.3	0xd1ec	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 1, 2021 13:31:44.120579958 CET	8.8.8.8	192.168.2.3	0xb976	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:44.120579958 CET	8.8.8.8	192.168.2.3	0xb976	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:44.220738888 CET	8.8.8.8	192.168.2.3	0x75b8	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Feb 1, 2021 13:31:44.220738888 CET	8.8.8.8	192.168.2.3	0x75b8	No error (0)	pastebin.com		104.23.99.190	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
Feb 1, 2021 13:29:16.645644903 CET	104.23.98.190	443	192.168.2.3	49713	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		
Feb 1, 2021 13:31:18.708425999 CET	104.23.99.190	443	192.168.2.3	49742	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		
Feb 1, 2021 13:31:42.537899971 CET	104.23.98.190	443	192.168.2.3	49746	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Feb 1, 2021 13:31:44.280311108 CET	104.23.98.190	443	192.168.2.3	49748	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 Mon Jan 27 13:46:39 CET 2020	Tue Aug 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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		
Feb 1, 2021 13:31:44.487889051 CET	104.23.98.190	443	192.168.2.3	49749	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 Mon Jan 27 13:46:39 CET 2020	Tue Aug 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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		

SMTP Packets

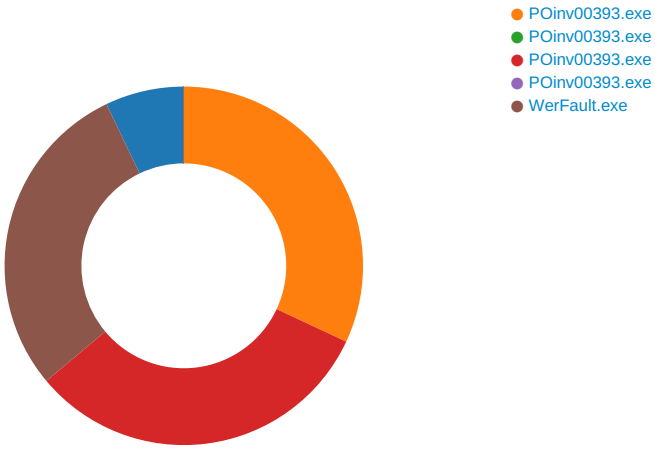
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 13:30:25.142040968 CET	587	49733	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 13:30:25.150007010 CET	49733	587	192.168.2.3	198.54.122.60	EHLO 878164
Feb 1, 2021 13:30:25.345933914 CET	587	49733	198.54.122.60	192.168.2.3	250-mta-14.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 13:30:25.387917042 CET	49733	587	192.168.2.3	198.54.122.60	STARTTLS
Feb 1, 2021 13:30:25.581036091 CET	587	49733	198.54.122.60	192.168.2.3	220 Ready to start TLS

Code Manipulations

Statistics

Behavior

- POinv00393.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- POinv00393.exe
- POinv00393.exe



Click to jump to process

System Behavior

Analysis Process: POinv00393.exe PID: 6708 Parent PID: 5692

General

Start time:	13:29:05
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\POinv00393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POinv00393.exe'
Imagebase:	0xe70000
File size:	4552704 bytes
MD5 hash:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.358061331.000000000744F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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\POinv00393.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	6CEFDD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CEFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\16654f11-3a02-4cab-b1ad-a4500300c0c5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	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	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POinv00393.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.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 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 73 55 17 60 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 50 00 00 dc 43 00 00 9a 01 00 00 00 00 00 ae fb 43 00 00 20 00 00 00 00 44 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 c0 45 00 00 02 00 00 00 00 00 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...sU.`.......... "...P...C...........C.. ....D. ..@.. .... E...........@.................	success or wait	9	6CEFDD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.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	6CEFDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POinv00393.exe.log	unknown	1039	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CEF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CEF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CEF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6CEF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6CEF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6CEF5F3C	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\POinv00393.exe	success or wait	1	6CEF646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\POinv00393.exe	dword	0	success or wait	1	6CEFC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	shell	unicode	explorer.exe,"C:\Users\user\Desktop\POinv00393.exe"	success or wait	1	6CEF646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	POinv00393.exe	unicode	C:\Users\user\Desktop\POinv00393.exe	success or wait	1	6CEF646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\POinv00393.exe	dword	0	success or wait	1	6CEFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6CEFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6CEFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6CEFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6CEFC075	RegSetValueExW

Analysis Process: powershell.exe PID: 6892 Parent PID: 6708

General

Start time:	13:29:14
Start date:	01/02/2021
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\POinv00393.exe' -Force
Imagebase:	0xcc0000
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:\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	6CE55B28	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	6CE55B28	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	6E0ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ap14tuqv.fkf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_btp5zmxs.mrt.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\Documents\20210201	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\Documents\20210201\PowerShell_transcript.878164.RU3nUHy1.20210201132916.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ap14tuqv.fkf.ps1	success or wait	1	6CEF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_btp5zmxs.mrt.psm1	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ap14tuqv.fkf.ps1	unknown	1	31	1	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_btp5zmxs.mrt.psm1	unknown	1	31	1	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\Documents\20210201\PowerShell_transcript.878164.RU3nUHy1.20210201132916.txt	unknown	3	ef bb bf	...	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\Documents\20210201\PowerShell_transcript.878164.RU3nUHy1.20210201132916.txt	unknown	730	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 32 30 31 31 33 32 39 34 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 68 61 72 64 7a 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 68 61 72 64 7a 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 38 37 38 31 36 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210201132945..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878164 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	30	6CEF1B4F	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 13 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	6CEF1B4F	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	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker.....Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal.....Unlock-PasswordInternal.....Unlock-BitLocker.....Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 e7 12 00 00 15 00 00 00 ea 0d 38 05 b2 08 a0 08 7e 08 00 00 00 00 9f 02 3d 00 c9 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....8...~.....=.....@.....	success or wait	1	6E3776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .::..... .	success or wait	16	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	16	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 37 26 00 01 5e 26 00 01 de 26 00 01 26 68 00	....T.@..>@...@.V.@.H .@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@.x T@.zT@..T @.=M@.DM@.:M@."M@. M@.!M@.;M@. .D@..D@.@M@. <M@.$M@.8M@.? M@.EM @..q...q...S...%...n..4&..5&. .7&..^&...&..&h.	success or wait	10	6E3776FC	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	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E08CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E091F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6E09203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	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	6CEF1B4F	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	6CEF1B4F	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	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	132	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEF1B4F	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	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	11	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6E06D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CEF1B4F	ReadFile

Analysis Process: conhost.exe PID: 6900 Parent PID: 6892

General

Start time:	13:29:14
Start date:	01/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 6916 Parent PID: 6708

General

Start time:	13:29:14
Start date:	01/02/2021
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\POinv00393.exe' -Force
Imagebase:	0xcc0000
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	6E0ACF06	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	6E0ACF06	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	6CE55B28	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	6CE55B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_3gd4shtk.lf5.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_q0eyjx0q.um5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\Documents\20210201\PowerShell_transcript.878164.c22VO1SZ.20210201132917.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	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	1	6CEF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_3gd4shtk.lf5.ps1	success or wait	1	6CEF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_q0eyjx0q.um5.psm1	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_3gd4shtk.lf5.ps1	unknown	1	31	1	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_q0eyjx0q.um5.psm1	unknown	1	31	1	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\Documents\20210201\PowerShell_transcript.878164.c22VO1SZ.20210201132917.txt	unknown	3	ef bb bf	...	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210201\PowerShell_transcript.878164.c22VO1SZ.20210201132917.txt	unknown	730	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 32 30 31 31 33 32 39 35 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 68 61 72 64 7a 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 68 61 72 64 7a 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 38 37 38 31 36 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	********************..Windows PowerShell transcript start..Start time: 20210201132953..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878164 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	30	6CEF1B4F	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	2	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	2	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2242	2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 4e 65 77 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 1c 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 46 69 6c 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 00 00 00 00 79 48 e2 38 ca 9f d5 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 64 31 17 00 00 00 08 00 00 00 44 65 73 63 72 69 62 65 02 00 00 00 11 00 00 00 47 65 74 2d 54 65 73 74 44 72 69 76 65 49 74 65 6d 02 00 00 00 0b 00 00 00 4e 65 77 2d 46 69 78	-AppLockerPolicy.....New-AppLockerPolicy.....Get-AppLockerPolicy.....Get-AppLockerFileInformation.....yH.8.....I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fix	success or wait	2	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e........Install-PackageProvider........Import-PackageProvider........Get-PackageProvider.........Register-PackageSource.........Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 f0 12 00 00 15 00 00 00 ea 0d dd 04 0d 09 f8 08 d6 08 00 00 00 00 60 01 20 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....`. .....@.....	success or wait	1	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.....:..... .	success or wait	16	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	16	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	6E3776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	....T.@..>@...@.V.@.H .@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@.x T@.zT@..T @.=M@.DM@.:M@."M@. M@.!M@.;M@. .D@..D@.@M@. <M@.$M@.8M..?M..BM ...D..mE..EM...q...q...S...%. ..n..4&..5&..7&.	success or wait	10	6E3776FC	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	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E08CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E091F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6E09203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	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	6CEF1B4F	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	6CEF1B4F	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	6CEF1B4F	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	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	116	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEF1B4F	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	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	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	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CEF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6E06D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CEF1B4F	ReadFile

Analysis Process: conhost.exe PID: 6964 Parent PID: 6916

General

Start time:	13:29:15
Start date:	01/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 6980 Parent PID: 6708

General

Start time:	13:29:15
Start date:	01/02/2021
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\POinv00393.exe' -Force
Imagebase:	0xcc0000
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	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_1jbb1rur.kxs.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_igqs5mg1.0fv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\Documents\20210201\PowerShell_transcr ipt.878164.GqBDotby.20210201132918.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_1jbb1rur.kxs.ps1	success or wait	1	6CEF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_igqs5mg1.0fv.psm1	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_1jbb1rur.kxs.ps1	unknown	1	31	1	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_igqs5mg1.0fv.psm1	unknown	1	31	1	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\Documents\20210201\PowerShell_transcr ipt.878164.GqBDotby.20210201132918.txt	unknown	3	ef bb bf	...	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\Documents\20210201\PowerShell_transcr ipt.878164.GqBDotby.20210201132918.txt	unknown	730	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 32 30 31 31 33 32 39 35 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 68 61 72 64 7a 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 68 61 72 64 7a 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 38 37 38 31 36 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	********************..Windo ws PowerShell transcript start..Start time: 20210201132952..Userna me: computer\user..RunAs User: computer\user..Configurati on Name: ..Machine: 878164 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	30	6CEF1B4F	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 13 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	2	6CEF1B4F	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	2	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e........Install-PackageProvider........Import-PackageProvider........Get-PackageProvider.........Register-PackageSource.........Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	2	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker........Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	2	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 f2 12 00 00 15 00 00 00 ea 0d 98 04 52 09 42 09 1f 09 00 00 00 00 94 02 3c 00 c9 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....R.B.....<.....@.....	success or wait	1	6E3776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3c 00 00 00 0e 00 20 00	H.....<@.^...L."My...:<..... .	success or wait	16	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	16	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	6E3776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 16 3b 40 01 ce 67 40 01 99 01 40 00 fb 00 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 1b 3b 40 01 3c 4d 40 01 24 4d 40 01 19 3b 40 01 38 4d 40 01 3f 4d 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 57 03 40 01 4d 03 40 01 42 4d 00	.....T.@..>@..;@..g@...@...@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT@..S@..S@..S@.\.@.T@..T@.@X@.?X@..T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@.M@.!M@.;M@..D@..D@.@M@..;@.<M@.$M@..;@.8M@.?M@..<@..<@..<@.W.@.M.@.BM.	success or wait	10	6E3776FC	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	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E08CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E091F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6E09203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	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	6CEF1B4F	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	6CEF1B4F	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	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEF1B4F	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	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	2	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E085705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6E06D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CEF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6CEF1B4F	ReadFile

Analysis Process: conhost.exe PID: 7072 Parent PID: 6980

General

Start time:	13:29:15
Start date:	01/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 7080 Parent PID: 6708

General

Start time:	13:29:15
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\Desktop\POinv00393.exe' -Force
Imagebase:	0xcc0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 7128 Parent PID: 7080

General

Start time:	13:29:16
Start date:	01/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: POinv00393.exe PID: 2100 Parent PID: 6708

General

Start time:	13:29:23
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\POinv00393.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\POinv00393.exe
Imagebase:	0x800000
File size:	4552704 bytes
MD5 hash:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: POinv00393.exe PID: 6464 Parent PID: 3388

General

Start time:	13:29:26
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\POinv00393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POinv00393.exe'
Imagebase:	0xe10000
File size:	4552704 bytes
MD5 hash:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: POinv00393.exe PID: 5436 Parent PID: 3388

General

Start time:	13:29:35
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\POinv00393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POinv00393.exe'
Imagebase:	0x780000
File size:	4552704 bytes
MD5 hash:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	low

Analysis Process: POinv00393.exe PID: 2296 Parent PID: 3388

General

Start time:	13:29:44
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\POinv00393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POinv00393.exe'
Imagebase:	0x110000
File size:	4552704 bytes
MD5 hash:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: POinv00393.exe PID: 1784 Parent PID: 3388

General

Start time:	13:29:52
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\POinv00393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POinv00393.exe'
Imagebase:	0xcc0000
File size:	4552704 bytes
MD5 hash:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: POinv00393.exe PID: 5404 Parent PID: 3388

General

Start time:	13:30:01
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\POinv00393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POinv00393.exe'
Imagebase:	0x740000
File size:	4552704 bytes
MD5 hash:	E0DB9D12220A5099BD1EBFEFC0CCDCFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: WerFault.exe PID: 5556 Parent PID: 2100

General

Start time:	13:30:26
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 1940
Imagebase:	0x370000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000003.446565112.00000000051F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000003.446565112.00000000051F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000003.446565112.00000000051F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Disassembly

Code Analysis