ID: 679457
Sample Name: BfwPdttqxH
Cookbook: default.jbs
Time: 20:23:10
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report BfwPdttqxH 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: AsyncRAT 5
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
System Summary 6
Data Obfuscation 6
Persistence and Installation Behavior 6
Boot Survival 6
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Lowering of HIPS / PFW / Operating System Security Settings 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\.exe.log 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BfwPdttqxH.exe.log 14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5dc33iso.2wh.ps1 14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qidwwvk3.wko.psm1 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t3bd04b3.uye.psm1 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yxtn0rnf.2ib.ps1 15
C:\Users\user\AppData\Local\Temp\tmp6E9F.tmp 15
C:\Users\user\AppData\Local\Temp\tmpD691.tmp 16
C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp.bat 16
C:\Users\user\AppData\Roaming\.exe 16
C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe 17
C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe:Zone.Identifier 17
C:\Users\user\Documents\20220805\PowerShell_transcript.216554.c1En_sl3.20220805202448.txt 17
C:\Users\user\Documents\20220805\PowerShell_transcript.216554.v9r7NV+a.20220805202421.txt 18
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 18
\Device\Null 18
Static File Info 19
General 19
File Icon 19
Static PE Info 19

General 19
Entrypoint Preview 19
Data Directories 21
Sections 22
Resources 22
Imports 22
Network Behavior 22
TCP Packets 22
Statistics 23
Behavior 24
System Behavior 24
Analysis Process: BfwPdttqxH.exePID: 5932, Parent PID: 5360 24
General 24
File Activities 24
Analysis Process: powershell.exePID: 1748, Parent PID: 5932 24
General 24
File Activities 25
File Created 25
File Deleted 25
File Written 25
File Read 27
Analysis Process: conhost.exePID: 3368, Parent PID: 1748 31
General 31
Analysis Process: schtasks.exePID: 2360, Parent PID: 5932 31
General 31
File Activities 31
File Read 31
Analysis Process: conhost.exePID: 5380, Parent PID: 2360 31
General 31
Analysis Process: BfwPdttqxH.exePID: 4684, Parent PID: 5932 32
General 32
Analysis Process: BfwPdttqxH.exePID: 1508, Parent PID: 5932 32
General 32
File Activities 32
File Created 32
File Written 33
File Read 33
Analysis Process: cmd.exePID: 5712, Parent PID: 1508 34
General 34
File Activities 34
Analysis Process: conhost.exePID: 4904, Parent PID: 5712 34
General 34
Analysis Process: cmd.exePID: 5684, Parent PID: 1508 34
General 34
File Activities 35
File Read 35
Analysis Process: schtasks.exePID: 4228, Parent PID: 5712 35
General 35
File Activities 35
Analysis Process: conhost.exePID: 5180, Parent PID: 5684 35
General 35
Analysis Process: timeout.exePID: 5784, Parent PID: 5684 36
General 36
File Activities 36
File Written 36
Analysis Process: .exePID: 4336, Parent PID: 5684 36
General 36
File Activities 36
File Created 36
File Deleted 37
File Written 37
File Read 38
Analysis Process: powershell.exePID: 916, Parent PID: 4336 38
General 38
Analysis Process: conhost.exePID: 1532, Parent PID: 916 39
General 39
Analysis Process: schtasks.exePID: 5236, Parent PID: 4336 39
General 39
Analysis Process: conhost.exePID: 3400, Parent PID: 5236 39
General 39
Analysis Process: .exePID: 4180, Parent PID: 4336 39
General 39
Analysis Process: .exePID: 3356, Parent PID: 4336 40
General 40
Analysis Process: MpCmdRun.exePID: 1508, Parent PID: 4952 40
General 40
Analysis Process: conhost.exePID: 2236, Parent PID: 1508 40
General 40
Disassembly 41

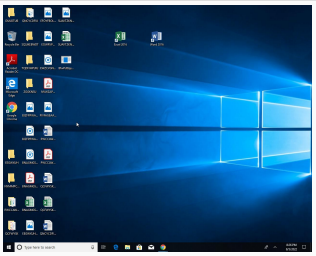
Windows Analysis Report

BfwPdttqxH

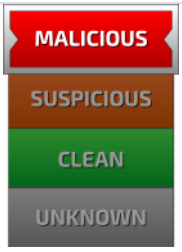
Overview

General Information

Sample Name:	BfwPdttqxH (renamed file extension from none to exe)
Analysis ID:	679457
MD5:	d4278af4c129db..
SHA1:	b6ca93a2c12c16..
SHA256:	9d19de1d4be447.
Tags:	32 exe trojan
Infos:	



Detection



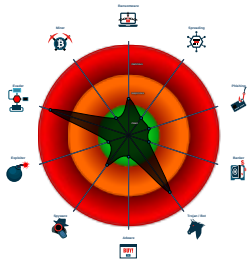
AsyncRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected AsyncRAT
- Multi AV Scanner detection for drop…
- Creates executable files without a n…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- BfwPdttqxH.exe (PID: 5932 cmdline: "C:\Users\user\Desktop\BfwPdttqxH.exe" MD5: D4278AF4C129DB3EA1C48D890304ABD1)
  - powershell.exe (PID: 1748 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2360 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZgolgcKGNozdg" /XML "C:\Users\user\AppData\Local\Temp\tmp6E9F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - BfwPdttqxH.exe (PID: 4684 cmdline: C:\Users\user\Desktop\BfwPdttqxH.exe MD5: D4278AF4C129DB3EA1C48D890304ABD1)
  - BfwPdttqxH.exe (PID: 1508 cmdline: C:\Users\user\Desktop\BfwPdttqxH.exe MD5: D4278AF4C129DB3EA1C48D890304ABD1)
    - cmd.exe (PID: 5712 cmdline: "C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "" /tr "'C:\Users\user\AppData\Roaming\.exe'" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 4904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 4228 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "" /tr "'C:\Users\user\AppData\Roaming\.exe'" MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 5684 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp.bat"" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 5784 cmdline: timeout 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - .exe (PID: 4336 cmdline: "C:\Users\user\AppData\Roaming\.exe" MD5: D4278AF4C129DB3EA1C48D890304ABD1)
        - powershell.exe (PID: 916 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 1532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 5236 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZgolgcKGNozdg" /XML "C:\Users\user\AppData\Local\Temp\tmpD691.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 3400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - .exe (PID: 4180 cmdline: C:\Users\user\AppData\Roaming\.exe MD5: D4278AF4C129DB3EA1C48D890304ABD1)
        - .exe (PID: 3356 cmdline: C:\Users\user\AppData\Roaming\.exe MD5: D4278AF4C129DB3EA1C48D890304ABD1)
    - conhost.exe (PID: 2236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MpCmdRun.exe (PID: 1508 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT


```
{
  "Server": "37.0.14.198",
  "Ports": "6161",
  "Version": "0.5.7B",
  "Autorun": "true",
  "Install_Folder": "%AppData%"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.298988477.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x166c6:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
00000009.00000002.298988477.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x140ff:$x1: AsyncRAT • 0x1413d:$x1: AsyncRAT
00000019.00000002.346637668.0000000002931000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000019.00000002.346637668.0000000002931000.00000004.00000800.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x1bd8f:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM • 0x290db:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM • 0x3a6ff:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
00000019.00000002.346637668.0000000002931000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Asyncrat_11a11ba1	unknown	unknown	• 0x1bcfd:$a1: /c schtasks /create /f /sc onlogon /rl highest /tn " • 0x29049:$a1: /c schtasks /create /f /sc onlogon /rl highest /tn " • 0x3a66d:$a1: /c schtasks /create /f /sc onlogon /rl highest /tn " • 0x1d094:$a2: Stub.exe • 0x1d124:$a2: Stub.exe • 0x2a3e0:$a2: Stub.exe • 0x2a470:$a2: Stub.exe • 0x3bf3c:$a2: Stub.exe • 0x3bfcc:$a2: Stub.exe • 0x1886f:$a3: get_ActivatePong • 0x25bbb:$a3: get_ActivatePong • 0x371df:$a3: get_ActivatePong • 0x1bf15:$a4: vmware • 0x29261:$a4: vmware • 0x3a885:$a4: vmware • 0x1bd8d:$a5: \nuR\noisreVtnerruC\swodniW\tfosorciM\erawtfoS • 0x290d9:$a5: \nuR\noisreVtnerruC\swodniW\tfosorciM\erawtfoS • 0x3a6fd:$a5: \nuR\noisreVtnerruC\swodniW\tfosorciM\erawtfoS • 0x19686:$a6: get_SslClient • 0x269d2:$a6: get_SslClient • 0x37ff6:$a6: get_SslClient
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.BfwPdttqxH.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
9.0.BfwPdttqxH.exe.400000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
9.0.BfwPdttqxH.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xa333:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM

Source	Rule	Description	Author	Strings
9.0.BfwPdttqxH.exe.400000.0.unpack	Windows_Trojan_Asyncrat_11a11ba1	unknown	unknown	• 0xa2a1:$a1: /c schtasks /create /f /sc onlogon /rl highest /tn " • 0xb638:$a2: Stub.exe • 0xb6c8:$a2: Stub.exe • 0x6e13:$a3: get_ActivatePong • 0xa4b9:$a4: vmware • 0xa331:$a5: \nuR\noisreVtnerruC\swodniW\tfosorciM\erawtfoS • 0x7c2a:$a6: get_SslClient
25.2..exe.294fda8.6.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 35 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected AsyncRAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Persistence and Installation Behavior

Creates executable files without a name

Boot Survival

Yara detected AsyncRAT

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

Malware Analysis System Evasion

Yara detected AntiVM3

Yara detected AsyncRAT

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

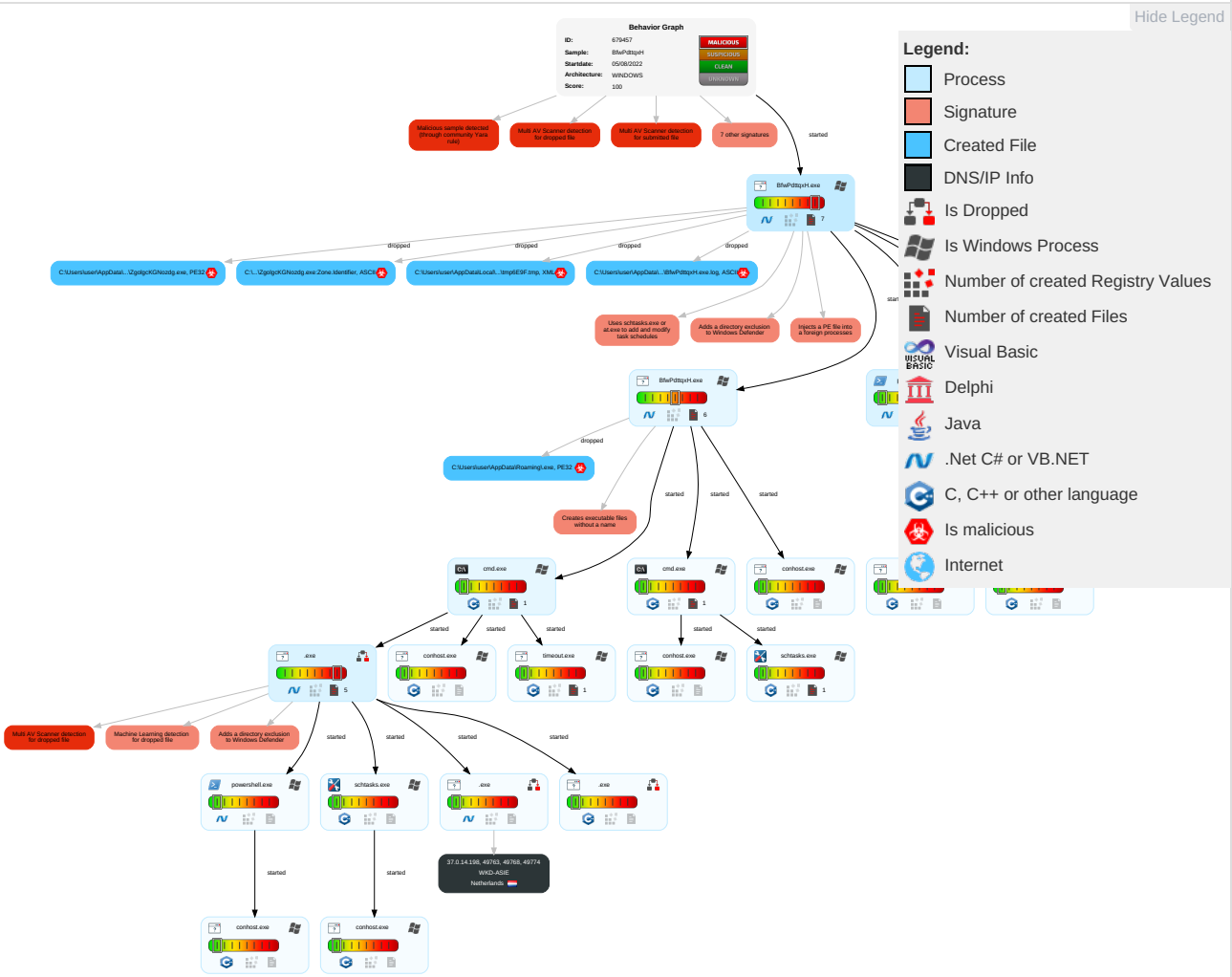
Lowering of HIPS / PFW / Operating System Security Settings

Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Scheduled Task/Job	2 Scheduled Task/Job	1 1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scripting	Boot or Logon Initialization Scripts	2 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Scripting	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
BfwPdttqxH.exe	24%	Virustotal		Browse
BfwPdttqxH.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\.exe	24%	Virustotal		Browse
C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe	24%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.BfwPdttqxH.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

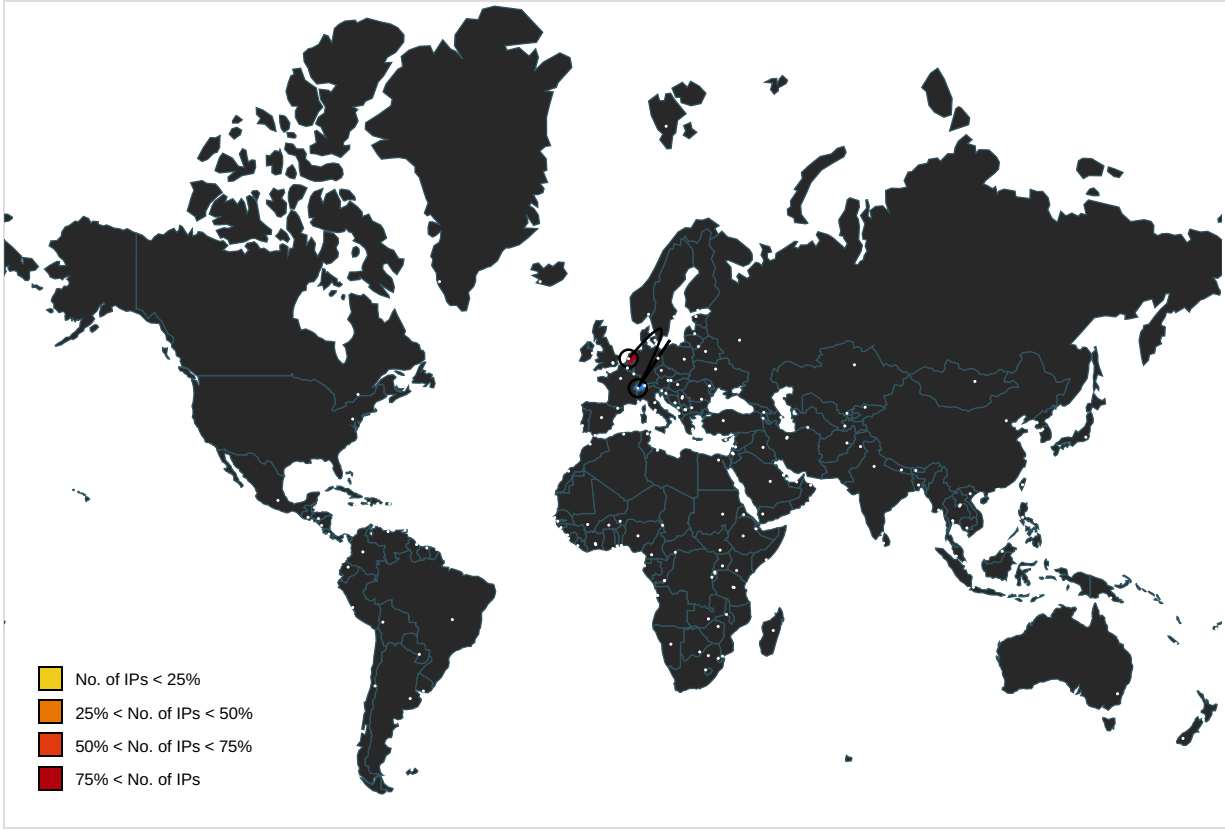
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	BfwPdttqxH.exe, 00000000.00000002.279559611.00000000028A7000.00000004.00000800.00020000.00000000.sdmp, BfwPdttqxH.exe, 00000009.00000002.299907239.0000000002AB5000.00000004.00000800.00020000.00000000.sdmp, .exe, 00000019.00000002.346146795.0000000028A9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	BfwPdttqxH.exe, 00000000.00000002.282781863.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.14.198	unknown	Netherlands		198301	WKD-ASIE	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679457
Start date and time: 05/08/202220:23:10	2022-08-05 20:23:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BfwPdttqxH (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@36/17@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target .exe, PID 3356 because it is empty
- Execution Graph export aborted for target BfwPdttqxH.exe, PID 1508 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:24:17	API Interceptor	1x Sleep call for process: BfwPdttqxH.exe modified
20:24:23	API Interceptor	83x Sleep call for process: powershell.exe modified
20:24:44	API Interceptor	1x Sleep call for process: .exe modified
20:25:43	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\.exe.log

Process:	C:\Users\user\AppData\Roaming\.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1750
Entropy (8bit):	5.3375092442007315

Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHYHKlEHUzvAHj:Pq5qXEwCYqhQnoPtIxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BfwPdttqxH.exe.log

Process:	C:\Users\user\Desktop\BfwPdttqxH.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1750
Entropy (8bit):	5.3375092442007315
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHYHKlEHUzvAHj:Pq5qXEwCYqhQnoPtIxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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):	22312
Entropy (8bit):	5.6017760530946585
Encrypted:	false
SSDEEP:	384:XtCDR7k0X8aiBQrnIS0nMjultI+HpaeQ99gRcxmT1MaLZlbAV7B/JcZBDI+Bo:ugBCITMCltxJat8RdCqfwtGVI
MD5:	706BF368BF41FC0C490878E2ADA9D7FB
SHA1:	9163B4C4C5C8B74749F97A632F1E417793FBBB5B
SHA-256:	087AA3BF3DD568E4E9D603F6913B584316B55D805CF2E6E359F9927CA720BEB8
SHA-512:	1E4D6DEE39B77F5E9515D218B9983C4E186866EF49D614CE06D33AF7ADAD8B9A77BCBE667F1268E9DEC68C2EB6636FADFE3000450FE1974B1E4E2511D70B9FE5
Malicious:	false
Preview:	@...e.....o.%.....T... .s.....@.....H.....<@.^.L."My...:P..... .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_5dc33iso.2wh.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qidwwvk3.wko.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t3bd04b3.uye.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yxtn0rnf.2ib.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp6E9F.tmp

Process:	C:\Users\user\Desktop\BfwPdttqxH.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.152940532036133
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtGxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTKv
MD5:	C1CE3B34B343D23210BE2315F10F6BD4
SHA1:	9F5FB230FF5A381EF31767BA6D63F8121D77EB43
SHA-256:	632E8FBEE2BEC3E0317733FF1F15F085C9F315DB7809DC1E47B86AE00C0E402F
SHA-512:	1BD66EE0E59FCF0814EB422A9A8F85BED743273B33409CA167DAB89DD8769CCC89D8B0D96F0F5820DFA923348286D0E8E85E828EB36E460189D1D6CA2ADF0EC7
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>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpD691.tmp

Process:	C:\Users\user\AppData\Roaming\.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.152940532036133
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtGxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTKv
MD5:	C1CE3B34B343D23210BE2315F10F6BD4
SHA1:	9F5FB230FF5A381EF31767BA6D63F8121D77EB43
SHA-256:	632E8FBEE2BEC3E0317733FF1F15F085C9F315DB7809DC1E47B86AE00C0E402F
SHA-512:	1BD66EE0E59FCF0814EB422A9A8F85BED743273B33409CA167DAB89DD8769CCC89D8B0D96F0F5820DFA923348286D0E8E85E828EB36E460189D1D6CA2ADF0EC7
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <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>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp.bat

Process:	C:\Users\user\Desktop\BfwPdttqxH.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	144
Entropy (8bit):	5.062292143444952
Encrypted:	false
SSDEEP:	3:mKDDCMNqTtvL5oWXp5cViEaKC50CSmqRDWXp5cViE2J5xAInTRIKWcoL1ZPy:hWKqTtT6WXp+NaZ50Zmq1WXp+N23fTrh
MD5:	20D2911EEB8394C37C85158E016A0465
SHA1:	FD49319833F2F4F14E56534A5BBF021C979E2701
SHA-256:	8AA8C51283BBAF49D7EC8CD207873285A89D982F06785828915D64DB1129244E
SHA-512:	D081F982072A7043887B85C6C502791AC9D8522C5FCD281814775CBD4082599D8103B0942B3660CF4EB1912E87929512CC8F60A6A52D820E30187850014D79BC
Malicious:	false
Preview:	@echo off..timeout 3 > NUL..START "" "C:\Users\user\AppData\Roaming\.exe"..CD C:\Users\user\AppData\Local\Temp\..DEL "tmpE3E2.tmp.bat" /f /q..

C:\Users\user\AppData\Roaming\.exe

Process:	C:\Users\user\Desktop\BfwPdttqxH.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	631296
Entropy (8bit):	7.350942080201485

Encrypted:	false
SSDEEP:	12288:AzTgQCM0ei0Hth5PSQ7OBOXhsAOf9vHg6SKlpx:tTAhPSkOBOPOf9vJLlpx
MD5:	D4278AF4C129DB3EA1C48D890304ABD1
SHA1:	B6CA93A2C12C164A73339020070662B618723744
SHA-256:	9D19DE1D4BE447775E3345EAE357A9571BD86A607EAF25DF48A6840ACBC390CC
SHA-512:	807C9A5242A831F2F70E8A949A11C58CFE79B9438A7C2D5484CE899CEF6F2F8574F7B03A8D896B5E6473669738266CB04B1B0F9C5E63D85C4C2A00E132B9DCC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 24%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F\.....0..... .....@.. ....@.....\...O.....@..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....@...PP.....$.....}.....(.....(.....{.....o.....*....0..w.....r...p..s.....~O.....o.....r$..p..B....(.....s.....o.....s. .....o.....{.....o.....&.....,..o.....*.....Tc.....]k.....0..:.....o .....,+..{....o!...o"....o#...o$....B.....(.....*...0..n.....r...p..s.....o.....r...p..B...(%.....(&.....B...('.....s.. ....o(.....r...p()...&...&.....,..o.....*.....KZ..

C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe

Process:	C:\Users\user\Desktop\BfwPdttqxH.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	631296
Entropy (8bit):	7.350942080201485
Encrypted:	false
SSDEEP:	12288:AzTgQCM0ei0Hth5PSQ7OBOXhsAOf9vHg6SKlpx:tTAhPSkOBOPOf9vJLlpx
MD5:	D4278AF4C129DB3EA1C48D890304ABD1
SHA1:	B6CA93A2C12C164A73339020070662B618723744
SHA-256:	9D19DE1D4BE447775E3345EAE357A9571BD86A607EAF25DF48A6840ACBC390CC
SHA-512:	807C9A5242A831F2F70E8A949A11C58CFE79B9438A7C2D5484CE899CEF6F2F8574F7B03A8D896B5E6473669738266CB04B1B0F9C5E63D85C4C2A00E132B9DCC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 24%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F\.....0..... .....@.. ....@.....\...O.....@..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....@...PP.....$.....}.....(.....(.....{.....o.....*....0..w.....r...p..s.....~O.....o.....r$..p..B....(.....s.....o.....s. .....o.....{.....o.....&.....,..o.....*.....Tc.....]k.....0..:.....o .....,+..{....o!...o"....o#...o$....B.....(.....*...0..n.....r...p..s.....o.....r...p..B...(%.....(&.....B...('.....s.. ....o(.....r...p()...&...&.....,..o.....*.....KZ..

C:\Users\user\AppData\Roaming\ZgolgcKGNozdg.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\BfwPdttqxH.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220805\PowerShell_transcript.216554.c1En_sl3.20220805202448.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):	5798
Entropy (8bit):	5.410872515008515
Encrypted:	false
SSDEEP:	96:BZYhdNwqDo1ZsZMhdNwqDo1Z3P5XjZwhdNwqDo1Z1innaZ9:G
MD5:	AF8EAD164BD6A94818BE40733782624B
SHA1:	86A8F8065E2DDA3E5DD7A9E8B2E35DA8B982CEA6

SHA-256:	0D5E2430B9431E5CC87FBF4E74FCA20AD1569A9CF266C57692DC80893D3E5488
SHA-512:	FB9BE0EFA1E576182ED86026C3DB44CE0497EAA68A5237A29B544688EBD3EFE9E2EF3735D8559EFCF225E80584D3460469922A97DE2C619A0AEC996189115E6 2
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20220805202449..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (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\ZgolgcKGNozdg.exe..Process ID: 916..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: 20220805202449..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppD ata\Roaming\ZgolgcKGNozdg.exe..**********************..Windows PowerShell transcript start..Start time: 20220805202904..Username: computer\user..RunAs User: com puter

C:\Users\user\Documents\20220805\PowerShell_transcript.216554.v9r7NV+a.20220805202421.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):	5801
Entropy (8bit):	5.411757839217602
Encrypted:	false
SSDEEP:	96:BZJhdNoqDo1Z5Z7hdNoqDo1Z9P5XjZdhdNoqDo1ZoinnvZA:X
MD5:	1A03A3E434CC299FA1E9A277DB8517E8
SHA1:	0BC8A930029AC6574616DE1BAD1F672938C35783
SHA-256:	F9B62836023539D552AF384A8100090FAE4C8590D2948D8501FC391639AD49DE
SHA-512:	54476AB7B23868ABCE8B089422B8A861F07D801BEACE33DA4E187BF11884CD71BD7A6BC99C0F27034A7EC41BD360C4293EA74201F7141D0EBE47C326AEF3E1 12
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20220805202422..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (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\ZgolgcKGNozdg.exe..Process ID: 1748..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: 20220805202422..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\App Data\Roaming\ZgolgcKGNozdg.exe..**********************..Windows PowerShell transcript start..Start time: 20220805202815..Username: computer\user..RunAs User: DE SKTOP-716T77

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.164173951604669
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zu+e:j+s+v+b+P+m+0+Q+q+F+e
MD5:	7348401F64247D0E1CBEFF9389397F09
SHA1:	29469747E7C077375051373F2353CB8C3332A73A
SHA-256:	7698074830824D745986D9499E756FB505C46118BEF38B3B3317D3572726C298
SHA-512:	8EA31EAE7D517653A0553402CF693975371793E0157FC20FA5715184248402BFFE807E698AF5926DC609D3E4EF7E8E5F983B8AFB037B03CB29C1A0A09CF4A1D8
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.41440934524794
Encrypted:	false
SSDEEP:	3:hYFqdLGAR+mQRKVxLZXt0sn:hYFqGaNZKsn
MD5:	3DD7DD37C304E70A7316FE43B69F421F
SHA1:	A3754CFC33E9CA729444A95E95BCB53384CB51E4
SHA-256:	4FA27CE1D904EA973430ADC99062DCF4BAB386A19AB0F8D9A4185FA99067F3AA

SHA-512:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0AAA4
Malicious:	false
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.350942080201485
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:	BfwPdttqxH.exe
File size:	631296
MD5:	d4278af4c129db3ea1c48d890304abd1
SHA1:	b6ca93a2c12c164a73339020070662b618723744
SHA256:	9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc
SHA512:	807c9a5242a831f2f70e8a949a11c58cfe79b9438a7c2d5484ce899cef6f2f8574f7b03a8d896b5e6473669738266cb04b1b0f9c5e63d85c4c2a00e132b9dcc2
SSDEEP:	12288:AzTgQCM0ei0Hth5PSQ7OBOXhsAOf9vHg6SKlpx:tTAhPSkOBOPOf9vJLlpx
TLSH:	52D40295B2EB9B23E9784FF2B42152644770A03F956BE24E5C893CFB55B1B134B80B43
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F\.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49b6ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x805C46C7 [Tue Mar 30 03:04:39 2038 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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]
dec eax
xor al, 46h
pop edx

Instruction
push esp
inc edi
inc ebx
pop eax
cmp byte ptr [edi], dh
pop eax
xor al, 38h
inc edx
inc esi
aaa
xor al, 47h
inc edx
xor eax, 00003838h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9b65c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9c000	0x5ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x9b640	0x1c	.text
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	0x996cc	0x99800	False	0.7814647165105864	data	7.355955012928353	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x5ec	0x600	False	0.4283854166666667	data	4.1832179829896345	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x9c090	0x35c	data		
RT_MANIFEST	0x9c3fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

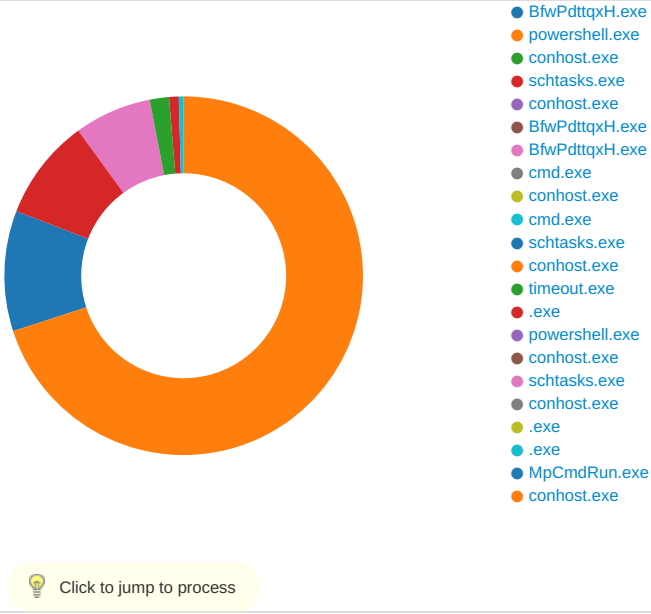
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 20:25:00.649559975 CEST	49763	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:00.677119970 CEST	6161	49763	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:01.218621969 CEST	49763	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:01.246222019 CEST	6161	49763	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:01.828075886 CEST	49763	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:01.855520010 CEST	6161	49763	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:06.867600918 CEST	49768	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:06.895004988 CEST	6161	49768	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:07.548412085 CEST	49768	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:07.575721979 CEST	6161	49768	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:08.094209909 CEST	49768	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:08.122539997 CEST	6161	49768	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:13.297027111 CEST	49774	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:13.324470043 CEST	6161	49774	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:13.985409021 CEST	49774	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:14.012593985 CEST	6161	49774	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:14.594739914 CEST	49774	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:14.622123003 CEST	6161	49774	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:19.653361082 CEST	49777	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:19.680777073 CEST	6161	49777	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:20.298470974 CEST	49777	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:20.326313972 CEST	6161	49777	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:20.985925913 CEST	49777	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:21.013403893 CEST	6161	49777	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:26.024643898 CEST	49779	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:26.052314043 CEST	6161	49779	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:26.642718077 CEST	49779	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:26.670074940 CEST	6161	49779	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:27.345860004 CEST	49779	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:27.373054981 CEST	6161	49779	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:32.378705025 CEST	49794	6161	192.168.2.3	37.0.14.198

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 20:25:32.406044006 CEST	6161	49794	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:32.987075090 CEST	49794	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:33.014451981 CEST	6161	49794	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:33.596462965 CEST	49794	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:33.623859882 CEST	6161	49794	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:38.629328012 CEST	49807	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:38.656769037 CEST	6161	49807	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:39.315737009 CEST	49807	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:39.343333006 CEST	6161	49807	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:39.932595015 CEST	49807	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:39.960140944 CEST	6161	49807	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:44.973624945 CEST	49814	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:45.000778913 CEST	6161	49814	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:45.504049063 CEST	49814	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:45.531956911 CEST	6161	49814	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:46.035042048 CEST	49814	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:46.062295914 CEST	6161	49814	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:51.068294048 CEST	49819	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:51.095670938 CEST	6161	49819	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:51.598002911 CEST	49819	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:51.625327110 CEST	6161	49819	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:52.129281044 CEST	49819	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:52.156703949 CEST	6161	49819	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:57.174474001 CEST	49833	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:57.201643944 CEST	6161	49833	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:57.707907915 CEST	49833	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:57.735132933 CEST	6161	49833	37.0.14.198	192.168.2.3
Aug 5, 2022 20:25:58.239228964 CEST	49833	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:25:58.266422987 CEST	6161	49833	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:03.272723913 CEST	49848	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:03.300067902 CEST	6161	49848	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:03.802263975 CEST	49848	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:03.829683065 CEST	6161	49848	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:04.333569050 CEST	49848	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:04.362463951 CEST	6161	49848	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:09.367032051 CEST	49849	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:09.394157887 CEST	6161	49849	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:09.896497965 CEST	49849	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:09.923904896 CEST	6161	49849	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:10.427694082 CEST	49849	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:10.455108881 CEST	6161	49849	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:15.459968090 CEST	49850	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:15.487970114 CEST	6161	49850	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:15.990724087 CEST	49850	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:16.018672943 CEST	6161	49850	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:16.522026062 CEST	49850	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:16.549967051 CEST	6161	49850	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:21.554250956 CEST	49852	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:21.581816912 CEST	6161	49852	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:22.084964037 CEST	49852	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:22.112504005 CEST	6161	49852	37.0.14.198	192.168.2.3
Aug 5, 2022 20:26:22.616478920 CEST	49852	6161	192.168.2.3	37.0.14.198
Aug 5, 2022 20:26:22.644006014 CEST	6161	49852	37.0.14.198	192.168.2.3

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: BfwPdttqxH.exe PID: **5932**, Parent PID: **5360**

General

Target ID:	0
Start time:	20:24:07
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\BfwPdttqxH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\BfwPdttqxH.exe"
Imagebase:	0x2c0000
File size:	631296 bytes
MD5 hash:	D4278AF4C129DB3EA1C48D890304ABD1
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: 00000000.00000002.279559611.00000000028A7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.279880645.0000000002933000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000002.279880645.0000000002933000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Asyncrat_11a11ba1, Description: unknown, Source: 00000000.00000002.279880645.0000000002933000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: **1748**, Parent PID: **5932**

General

Target ID:	4
Start time:	20:24:20
Start date:	05/08/2022
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\ZgolgcKGNozdg.exe
Imagebase:	0x950000

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	6CDFCF06	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	6CDFCF06	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	6BBA5B28	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	6BBA5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5dc33iso.2wh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BC41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qidwwvk3.wko.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BC41E60	CreateFileW
C:\Users\user\Documents\20220805	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BC4BEFF	CreateDirectoryW
C:\Users\user\Documents\20220805\PowerShell_transcript.216554.v9r7NV+a.20220805202421.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BC41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5dc33iso.2wh.ps1	success or wait	1	6BC46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qidwwvk3.wko.psm1	success or wait	1	6BC46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBA5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBA5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBA5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBA5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBA5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBA5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBA5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5dc33iso.2wh.ps1	0	1	31	1	success or wait	1	6BC41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qidwwvk3.wko.psm1	0	1	31	1	success or wait	1	6BC41B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.216554.v9r7NV+a.20220805202421.txt	0	3	ff		success or wait	1	6BC41B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.216554.v9r7NV+a.20220805202421.txt	3	680	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 32 30 38 30 35 32 30 32 34 32 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220805202422Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 216554 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6BC41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 14 00 00 19 00 00 00 fd 0d 6f 05 25 08 1a 08 1a 08 00 00 54 00 fd 00 20 00 73 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eo%T s@	success or wait	1	6D0C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6D0C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D0C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6D0C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6D0C76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 09 09 fd 00 00 54 40 01 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 00 01 19 3b 00 01 fd 3c 00 01 fd 3c 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@ S@\@T@Xd@Vd@*@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@;BMDmE;; <<	success or wait	11	6D0C76FC	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	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CDDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CDE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22388	success or wait	1	6CDE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	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	6BC41B4F	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	6BC41B4F	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	6BC41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CDD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BC41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BC41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BC41B4F	ReadFile

Analysis Process: conhost.exe PID: **3368**, Parent PID: **1748**

General

Target ID:	5
Start time:	20:24:20
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: **2360**, Parent PID: **5932**

General

Target ID:	6
Start time:	20:24:20
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZgolgcKGNozdg" /XML "C:\Users\user\AppData\Local\Temp\tmp6E9F.tmp
Imagebase:	0xab0000
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\tmp6E9F.tmp	unknown	2	success or wait	1	ABAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6E9F.tmp	unknown	1601	success or wait	1	ABABD9	ReadFile

Analysis Process: conhost.exe PID: **5380**, Parent PID: **2360**

General

Target ID:	7
Start time:	20:24:21
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: BfwPdttqxH.exe PID: **4684**, Parent PID: **5932**

General

Target ID:	8
Start time:	20:24:24
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\BfwPdttqxH.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\BfwPdttqxH.exe
Imagebase:	0x2b0000
File size:	631296 bytes
MD5 hash:	D4278AF4C129DB3EA1C48D890304ABD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BfwPdttqxH.exe PID: **1508**, Parent PID: **5932**

General

Target ID:	9
Start time:	20:24:25
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\BfwPdttqxH.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BfwPdttqxH.exe
Imagebase:	0x6f0000
File size:	631296 bytes
MD5 hash:	D4278AF4C129DB3EA1C48D890304ABD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000009.00000002.298988477.0000000002A31000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000009.00000002.298988477.0000000002A31000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000009.00000002.307316402.0000000005006000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000009.00000000.273890035.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000009.00000000.273890035.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDFCF06	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	6CDFCF06	unknown
C:\Users\user\AppData\Roaming\.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BC41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BC47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BC41E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\.exe	0	631296	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 46 5c fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 09 00 00 08 00 00 00 00 00 00 fd fd 09 00 00 20 00 00 00 fd 09 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 00 0a 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELF\0 @ @	success or wait	1	6BC41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp.bat	0	144	40 65 63 68 6f 20 6f 66 66 0d 0a 74 69 6d 65 6f 75 74 20 33 20 3e 20 4e 55 4c 0d 0a 53 54 41 52 54 20 22 22 20 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 2e 65 78 65 22 0d 0a 43 44 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 0d 0a 44 45 4c 20 22 74 6d 70 45 33 45 32 2e 74 6d 70 2e 62 61 74 22 20 2f 66 20 2f 71 0d 0a	@echo offtimeout 3 > NULSTART "" "C:\Users\user\AppData\Roaming\.exe"CD C:\Users\user\AppData\Local\Temp\DEL "tmpE3E2.tmp.bat" /f /q	success or wait	1	6BC41B4F	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	6CDD5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Users\user\Desktop\BfwPdttqxH.exe	unknown	631296	success or wait	1	6BC41B4F	ReadFile

Analysis Process: cmd.exe PID: **5712**, Parent PID: **1508**

General

Target ID:	14
Start time:	20:24:34
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "" /tr "'C:\Users\user\AppData\Roaming\.exe'" & exit
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4904**, Parent PID: **5712**

General

Target ID:	16
Start time:	20:24:34
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **5684**, Parent PID: **1508**

General

Target ID:	17
Start time:	20:24:34

Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp.bat""
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE3E2.tmp.bat	unknown	8191	success or wait	5	C2FB07	ReadFile

Analysis Process: schtasks.exe PID: **4228**, Parent PID: **5712**

General

Target ID:	18
Start time:	20:24:34
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn "" /tr '"C:\Users\user\AppData\Roaming\.exe"'
Imagebase:	0xab0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5180**, Parent PID: **5684**

General

Target ID:	20
Start time:	20:24:35
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: **5784**, Parent PID: **5684**

General

Target ID:	22
Start time:	20:24:36
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0x13b0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	15	15	20 73 65 63 6f 6e 64 73 2c 20 70 72 65 73 73	seconds, press	success or wait	1	13B2DA7	fprintf
\Device\Null	52	37	08 32 08 31 08 30 0d 0a	210	success or wait	1	13B2DA7	fprintf
\Device\Null	54	2	08 31	1	success or wait	3	13B2DA7	fprintf
\Device\Null	60	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	13B2DA7	fprintf

Analysis Process: .exe PID: **4336**, Parent PID: **5684**

General

Target ID:	25
Start time:	20:24:40
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Roaming\.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\.exe"
Imagebase:	0x360000
File size:	631296 bytes
MD5 hash:	D4278AF4C129DB3EA1C48D890304ABD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000019.00000002.346637668.0000000002931000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000019.00000002.346637668.0000000002931000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Asyncrat_11a11ba1, Description: unknown, Source: 00000019.00000002.346637668.0000000002931000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000019.00000002.346146795.00000000028A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, Virustotal, Browse

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDFCF06	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	6CDFCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpD691.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BC47038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D10C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD691.tmp	success or wait	1	6BC46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD691.tmp	0	1600	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 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 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 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 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 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?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>	success or wait	1	6BC41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\.exe.log	0	1750	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 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 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 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D10C907	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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6CD303DE	ReadFile

Analysis Process: powershell.exe PID: **916**, Parent PID: **4336**

General

Target ID:	29
Start time:	20:24:46
Start date:	05/08/2022
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\ZgolgcKGNozdg.exe
Imagebase:	0x950000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

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

Analysis Process: conhost.exe PID: **1532**, Parent PID: **916**

General	
Target ID:	30
Start time:	20:24:47
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5236**, Parent PID: **4336**

General	
Target ID:	31
Start time:	20:24:47
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZgolgcKGNozdg" /XML "C:\Users\user\AppData\Local\Temp\tmpD691.tmp
Imagebase:	0xab0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3400**, Parent PID: **5236**

General	
Target ID:	32
Start time:	20:24:48
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: .exe PID: **4180**, Parent PID: **4336**

General

Target ID:	34
Start time:	20:24:51
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Roaming\.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\.exe
Imagebase:	0x3d0000
File size:	631296 bytes
MD5 hash:	D4278AF4C129DB3EA1C48D890304ABD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: .exe PID: **3356**, Parent PID: **4336**

General

Target ID:	35
Start time:	20:24:52
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Roaming\.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\.exe
Imagebase:	0x470000
File size:	631296 bytes
MD5 hash:	D4278AF4C129DB3EA1C48D890304ABD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000023.00000002.518564468.0000000004F98000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000023.00000002.507915414.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000023.00000002.507915414.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen

Analysis Process: MpCmdRun.exe PID: **1508**, Parent PID: **4952**

General

Target ID:	43
Start time:	20:25:42
Start date:	05/08/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2236**, Parent PID: **1508**

General

Target ID:	44
Start time:	20:25:42
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly