ID: 877005
Sample Name: kdsyitkxmS.exe
Cookbook: default.jbs
Time: 11:18:06
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

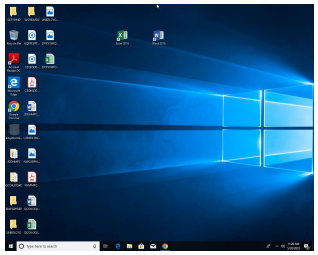
Windows Analysis Report

kdsyitkxmS.exe

Overview

General Information

Sample Name:	kdsyitkxmS.exe
Original Sample Name:	01fe6ba28d821..
Analysis ID:	877005
MD5:	01fe6ba28d821..
SHA1:	45748a6d6474...
SHA256:	626df082c2624..
Tags:	32 exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

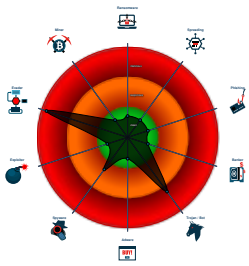
Glupteba

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected Glupteba
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Uses netsh to modify the Windows …
- Found Tor onion address
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Creates files in the system32 config…

Classification



Process Tree

- **System is w10x64**
- kdsyitkxmS.exe (PID: 4652 cmdline: C:\Users\user\Desktop\kdsyitkxmS.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
  - powershell.exe (PID: 5948 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kdsyitkxmS.exe (PID: 3320 cmdline: C:\Users\user\Desktop\kdsyitkxmS.exe MD5: 01FE6BA28D82175D35665B3EB6ED8CEA)
    - powershell.exe (PID: 7000 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5952 cmdline: C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - netsh.exe (PID: 2576 cmdline: netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes MD5: 98CC37BBF363A38834253E22C80A8F32)
    - powershell.exe (PID: 2080 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4820 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 1812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Glupteba	Glupteba is a trojan horse malware that is one of the top ten malware variants of 2021. After infecting a system, the Glupteba malware can be used to deliver additional malware, steal user authentication information, and enroll the infected system in a cryptomining botnet.	No Attribution	http://resources.infosecinstitute.com/tdss4-part-1/https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/https://blog.google/technology/safety-security/new-action-combat-cyber-crime/https://blog.google/threat-analysis-group/disrupting-glupteba-operation/https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.glupteba

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.374126530.00000000030C0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000002.367355865.0000000004400000.00000040.00000001.01000000.00000003.sdmp	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth (Nextron Systems)	• 0x3b8597:$x1: https://cdn.discordapp.com/attachments/
00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth (Nextron Systems)	• 0x3b7997:$x1: https://cdn.discordapp.com/attachments/
00000005.00000002.622953381.0000000002B35000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x798:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000005.00000002.619390815.0000000004400000.00000040.00000001.01000000.00000003.sdmp	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth (Nextron Systems)	• 0x3b8597:$x1: https://cdn.discordapp.com/attachments/
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.kdsyitkxmS.exe.3e41700.0.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x39858:$s2: The Magic Word! • 0x45998:$s2: The Magic Word! • 0x39bb8:$s3: Software\Oracle\VirtualBox • 0x39847:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
0.2.kdsyitkxmS.exe.a1cb00.7.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x3f458:$s2: The Magic Word! • 0x4b598:$s2: The Magic Word! • 0x3f7b8:$s3: Software\Oracle\VirtualBox • 0x3f447:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73

Source	Rule	Description	Author	Strings
0.3.kdsyitkxmS.exe.3fcbb00.5.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x3f458:$s2: The Magic Word! • 0x4b598:$s2: The Magic Word! • 0x3f7b8:$s3: Software\Oracle\VirtualBox • 0x3f447:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
5.2.kdsyitkxmS.exe.3552567.10.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x39858:$s2: The Magic Word! • 0x45998:$s2: The Magic Word! • 0x39bb8:$s3: Software\Oracle\VirtualBox • 0x39847:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
0.2.kdsyitkxmS.exe.36f2287.10.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x29b38:$s2: The Magic Word! • 0x35c78:$s2: The Magic Word! • 0x29e98:$s3: Software\Oracle\VirtualBox • 0x29b27:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
Click to see the 25 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

Yara detected Glupteba

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Bitcoin Miner

Yara detected Glupteba

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Found Tor onion address

E-Banking Fraud

Yara detected Glupteba

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Creates files in the system32 config directory

Malware Analysis System Evasion

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

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information

Yara detected Glupteba

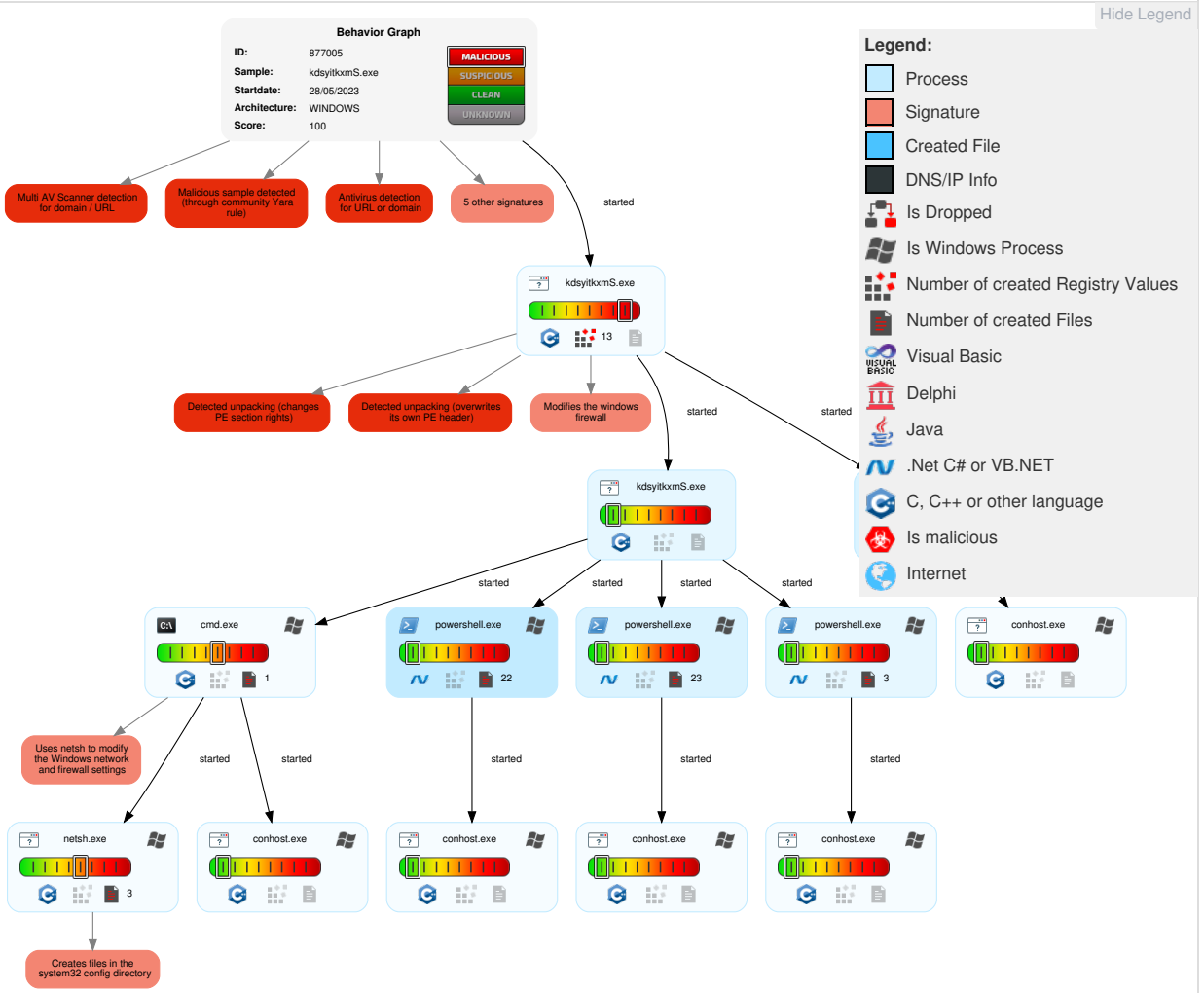
Remote Access Functionality

Yara detected Glupteba

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 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 1 1 Masquerading	1 Input Capture	1 3 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Proxy	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Disable or Modify Tools	LSASS Memory	4 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	4 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	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 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 Obfuscated Files or Information	LSA Secrets	1 2 System Information 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	2 Software Packing	Cached Domain Credentials	System Owner/User 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 File Deletion	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

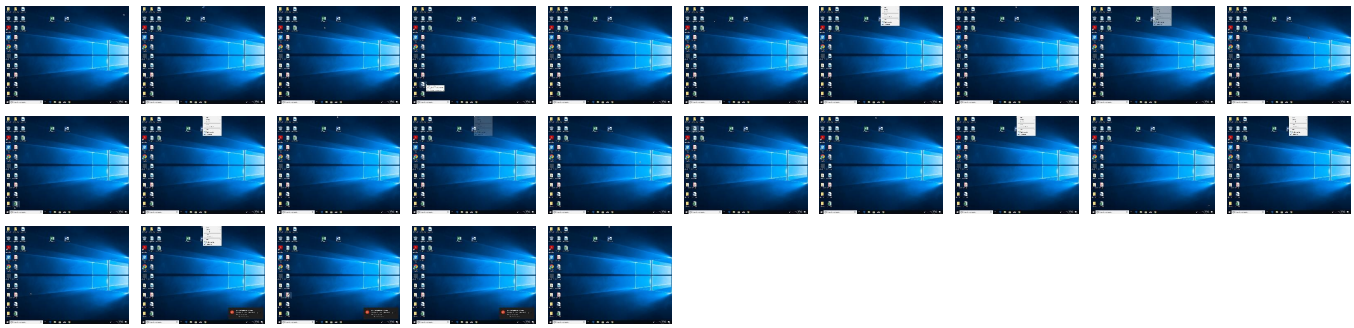
Behavior Graph



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
kdsyitkxmS.exe	32%	ReversingLabs		
kdsyitkxmS.exe	32%	Virustotal		Browse
kdsyitkxmS.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.spidersoft.com)Wg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://gais.cs.ccu.edu.tw/robot.php)Gulper	0%	URL Reputation	safe	
http://devlog.gregarius.net/docs/ua)Links	0%	URL Reputation	safe	
http://www.google.	0%	URL Reputation	safe	
http://www.exabot.com/go/robot)Opera/9.80	0%	URL Reputation	safe	
http://www.googlebot.com/bot.html)Links	0%	URL Reputation	safe	
http://www.alltheweb.com/help/webmaster/crawler)Mozilla/5.0	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://misc.yahoo.com.cn/help.html)QueryPerformanceFrequency	0%	URL Reputation	safe	
http://crl.g	0%	URL Reputation	safe	
http://https://blockchain.infoindex	0%	URL Reputation	safe	
http://https://duniadekho.barhttps://duniadekho.barRegQueryValueExWUUIDPGDSE64-bitc:	0%	Avira URL Cloud	safe	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionC:	0%	Avira URL Cloud	safe	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionS-1-5-21-3853321935-2125563209-	0%	Avira URL Cloud	safe	
http://invalidlog.txtlookup	0%	Avira URL Cloud	safe	
http://https://duniadekho.bar	100%	Avira URL Cloud	malware	
http://grub.org)Mozilla/5.0	0%	Avira URL Cloud	safe	
http://https://duniadekho.bar	20%	Virustotal		Browse
http://https://raw.githubusercontent.com/spesmilo/electrum/master/electrum/servers.jsonsize	0%	Avira URL Cloud	safe	
http://www.bloglines.com)Frame	0%	Avira URL Cloud	safe	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	100%	Avira URL Cloud	malware	
http://https://go.microT	0%	Avira URL Cloud	safe	
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionCommonPro	0%	Avira URL Cloud	safe	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.oniontls:	0%	Avira URL Cloud	safe	
http://https://duniadekho.barMicrosoft	0%	Avira URL Cloud	safe	
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionhttps://d	0%	Avira URL Cloud	safe	
http://https://_bad_pdb_file.pdb	0%	Avira URL Cloud	safe	
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	0%	Avira URL Cloud	safe	
http://https://duniadekho.barhttps://duniadekho.barRegQueryValueExWhttps://duniadekho.barUUIDUUIDPGDSEPGDSE	0%	Avira URL Cloud	safe	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionhttp://vcr4vuv4sf5233btfy7xboez	0%	Avira URL Cloud	safe	
http://www.avantbrowser.com)MOT-V9mm/00.62	0%	Avira URL Cloud	safe	
http://localhost:3433/https://duniadekho.baridna:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.spidersoft.com)Wg	kdsyitkxmS.exe	false	• Avira URL Cloud: safe	low
http://yandex.com/	kdsyitkxmS.exe	false		high
http://https://duniadekho.barhttps://duniadekho.barRegQueryValueExWUUIDPGDSE64-bitc:	kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C08E000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://search.msn.com/msnbot.htm)net/htt	kdsyitkxmS.exe	false		high
http://invalidlog.txtlookup	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.6193908 15.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://gais.cs.ccu.edu.tw/robot.php)Gulper	kdsyitkxmS.exe	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duniadekho.bar	kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C096000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C088000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C094000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C08E000.00000004.00001000.00020000.00000000.sdmp	true	• 20%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionC:	kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C0E4000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://devlog.gregarius.net/docs/ua)Links	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.google.	kdsyitkxmS.exe	false	• URL Reputation: safe	unknown
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionS-1-5-21-3853321935-2125563209-	kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C0DA000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://grub.org)Mozilla/5.0	kdsyitkxmS.exe	false	• Avira URL Cloud: safe	low
http://https://raw.githubusercontent.com/spesmilo/electrum/master/electrum/servers.jsonsize	kdsyitkxmS.exe	false	• Avira URL Cloud: safe	unknown
http://https://turnitin.com/robot/crawlerinfo.html)cannot	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false		high
http://www.exabot.com/go/robot)Opera/9.80	kdsyitkxmS.exe	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000B.00000002.514376329.0000000005231000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000F.00000002.622138820.00000000051F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.bloglines.com)Frame	kdsyitkxmS.exe	false	• Avira URL Cloud: safe	low
http://www.googlebot.com/bot.html)Links	kdsyitkxmS.exe	false	• URL Reputation: safe	unknown
http://search.msn.com/msnbot.htm)net/http:	kdsyitkxmS.exe, 00000000.00000002.374126530.00000000030C0000.00000040.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000000.00000002.367355865.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000000.00000003.353503298.00000000039B0000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false		high
http://www.alltheweb.com/help/webmaster/crawler)Mozilla/5.0	kdsyitkxmS.exe	false	• URL Reputation: safe	unknown
http://https://go.microT	powershell.exe, 0000000B.00000003.473426279.0000000005BE6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000B.00000002.514376329.0000000005369000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000B.00000003.490620541.0000000008071000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000B.00000003.480261495.0000000008062000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C096000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C0DE000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C0DA000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000B.00000002.514376329.0000000005369000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000B.00000003.490620541.0000000008071000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000B.00000003.480261495.0000000008062000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.google.com/bot.html)crypto/ecdh:	kdsyitkxmS.exe	false		high
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.oniontls:	kdsyitkxmS.exe	true	• Avira URL Cloud: safe	unknown
http://https://github.com/Snawoot/opera-proxy/releases/download/v1.2.2/opera-p	kdsyitkxmS.exe	false		high
http://search.msn.com/msnbot.htm)msnbot/1.1	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F3000.00000040.00001000.00020000.00000000.sdmp	false		high
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionCommonPro	kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C0E6000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C0E2000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://duniadekho.barMicrosoft	kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C094000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C09C000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.archive.org/details/archive.org_bot)Opera/9.80	kdsyitkxmS.exe	false		high
http://www.baidu.com/search/spider.htm)MobileSafari/600.1.4	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F3000.00000040.00001000.00020000.00000000.sdmp	false		high
http://yandex.com/bots)Opera/9.51	kdsyitkxmS.exe	false		high
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionhttps://d	kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C096000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.google.com/bot.html)Mozilla/5.0	kdsyitkxmS.exe	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000000B.00000002.514376329.0000000005369000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000B.00000003.490620541.0000000008071000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000B.00000003.480261495.0000000008062000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://_bad_pdb_file.pdb	kdsyitkxmS.exe, 00000000.00000002.374126530.000000000378B000.00000040.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000000.00000002.367355865.0000000000ACC000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000ACC000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.00000000035FB000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://archive.org/details/archive.org_bot)Mozilla/5.0	kdsyitkxmS.exe	false		high
http://https://duniadekho.barvcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onion	kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C0E4000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://misc.yahoo.com.cn/help.html)QueryPerformanceFrequency	kdsyitkxmS.exe	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://help.yahoo.com/help/us/ysearch/slurp)SonyEricssonK550i/R1JD	kdsyitkxmS.exe	false		high
http://www.avantbrowser.com	kdsyitkxmS.exe	false		high
http://https://duniadekho.barhttps://duniadekho.barRegQueryValueExWhttps://duniadekho.barUUIDUUIDPGDSEPGDSE	kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C088000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.google.com/feedfetcher.html)HKLM	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/attachments/1087398815188910163/1087399133926674453/LZ.zipreflect.Value.I	kdsyitkxmS.exe	false		high
http://crl.g	kdsyitkxmS.exe, 00000000.00000002.370479632.0000000002CC1000.00000040.00000020.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.622953381.0000000002B35000.00000040.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://blockchain.infoindex	kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.avantbrowser.com)MOT-V9mm/00.62	kdsyitkxmS.exe, 00000000.00000002.374126530.00000000030C0000.00000040.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000000.00000002.367355865.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000000.00000003.353503298.00000000039B0000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.onionhttp://vcr4vuv4sf5233btfy7xboez	kdsyitkxmS.exe, 00000000.00000002.378631978.000000000C0DE000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.628942791.000000000C0DA000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://localhost:3433/https://duniadekho.baridna:	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://search.msn.com/msnbot.htm)pkcs7:	kdsyitkxmS.exe, kdsyitkxmS.exe, 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, kdsyitkxmS.exe, 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, kdsyitkxmS.exe, 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp	false		high
http://www.alexa.com/help/webmasters;	kdsyitkxmS.exe	false		high
http://www.google.com/adsbot.html)Encountered	kdsyitkxmS.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877005

Start date and time:	2023-05-28 11:18:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
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
Sample file name:	kdsyitkxmS.exe
Original Sample Name:	01fe6ba28d82175d35665b3eb6ed8cea.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@19/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15.9% (good quality ratio 7.6%) • Quality average: 40.1% • Quality standard deviation: 44.2%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, TrustedInstaller.exe
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
11:18:58	API Interceptor	7x Sleep call for process: kdsyitkxmS.exe modified
11:19:01	API Interceptor	57x Sleep call for process: powershell.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\Windows\PowerShell\StartupProfileData-Interactive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22112
Entropy (8bit):	5.458574769940964
Encrypted:	false
SSDEEP:	384:PtCRjm27UAxOi7wRSVud7KjrPs5a1QQ1O5SeK8vH4e60CUXrNpipUW:sT7NES6Uud7uPQPXP4JDup2
MD5:	3634790B93223C11F6823442769CD2DE
SHA1:	404532205A20742419AD10578C279EDC2655E951
SHA-256:	0363B7D8D80C958BB9C3449F9E6F6AD754B263FDE1530B4E916CB0F1C5FB58D1
SHA-512:	70F7A6D71319E0C59719D1D34F0D325F08F585274A95EA642B9D52C1BB02687767D86C7C79D34AD70F42C04396C65FF0AA452115594B782125B48E292C39E68B
Malicious:	false
Preview:	@...e.....P.....H.....<@.^.L."My...:I..... .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_p030yzvi.tqg.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_zon3rn2d.2u2.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:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22096
Entropy (8bit):	5.598969772245669
Encrypted:	false
SSDEEP:	384:hYtCRvq0a9pk00X+p3eB4Exb9zFfjE8xea5cc7QQgSeFycB4Iz60vB0GpiOUB:uk0g4Exb5B5xTVqee4JkpO
MD5:	34C3603404E2348EB7B24B0F5E0B55D8
SHA1:	881BCB253515B12F17A11F8E35FE48AA1D38C8C0
SHA-256:	FC7B7585CDB3CF4601034A79EBE7993A18A4C3763AA9D4B0CDF850E2BE562A44
SHA-512:	EF1A4BAB154356C2224BEEF1B57B0462090072928B75A41B89FD69BB0D1C3BB234F8AFB27B59F933E4703352F5C3F9B1B8B8716454164DE74B67CDD4FEF2431 D
Malicious:	false
Preview:	@...e.....L.....5."."....4.....@.....H.....<@.^.L."My...:I..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Windows\Temp__PSScriptPolicyTest_1depap5s.43l.psm1

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

C:\Windows\Temp__PSScriptPolicyTest_fil3vomk.kwi.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_mfqj4tng.2eo.psm1

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

C:\Windows\Temp__PSScriptPolicyTest_uyxuby1g.134.ps1

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.97472217525508
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	kdsyitkxmS.exe
File size:	4379008
MD5:	01fe6ba28d82175d35665b3eb6ed8cea

SHA1:	45748a6d6474f470d44e848596e0e08bce674996
SHA256:	626df082c2624d9530794881921094aa100fa0a805b1544112d5a07dbe12cbc2
SHA512:	e1537b4ebf7dd9cf345b0f8c0646de1df1152469151b43cc8c08370eb3c40393940598de98a11e47c9810d891942f385f7c6cb9ad4470a3c8941961b2a98247b
SSDEEP:	98304:/RKU80KHe0iz3Dt6Ds6DV8G66EjKN69i5SvbFOqRrLfO2FnC86:/4e0i7Dt6XDGG/EjKN6LjxdFnC86
TLSH:	BB162313A3A1BD54E9564BB39F2F92F8776EB6708F143755311DBA1B08B02B2C263B11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Richb.....PE..L.....a.....

File Icon

Icon Hash:	454549495545611d

Static PE Info

General

Entrypoint:	0x404e59
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x61AADEB8 [Sat Dec 4 03:21:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2d9ed3462f8a74bfd1231e2e9de56b43

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=522a29533d3f200e2d1728300c14102108163131362632102304 2b113f2d26353224, PostalCode=10802, S=0b1c1115005f5c4e11160b0a090100180d1c4f170217 + S=0b1c1115494a5c17161151151d13510003465346500717 0e1c520b071c040f0f5216050f1244171f0b110e04061211081e0347124308570a1e0c0b195 a055b0c0b0a070b
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/28/2023 1:13:44 AM 5/27/2024 1:13:44 AM
Subject Chain	• CN=522a29533d3f200e2d1728300c14102108163131362632102304 2b113f2d26353224, PostalCode=10802, S=0b1c1115005f5c4e11160b0a090100180d1c4f170217 + S=0b1c1115494a5c17161151151d13510003465346500717 0e1c520b071c040f0f5216050f1244171f0b110e04061211081e0347124308570a1e0c0b 9560a055b0c0b0a070b
Version:	3
Thumbprint MD5:	FA499CD6C5F7A74F5A748B778F305AE3
Thumbprint SHA-1:	FF3C70A0D6A66705568453AA262257D22183BCA7
Thumbprint SHA-256:	F96E2C83FF581F02D48E26B51B960B61592EE9B397B86A2A3A604587ABC9D0B4
Serial:	10F68FF5E99D28F7644E5B17DA75165E

Entrypoint Preview

Instruction
call 00007F5C50D96D73h
jmp 00007F5C50D9240Dh
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F5C50D925B6h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F5C50D925E0h
test ecx, 00000003h
jne 00007F5C50D92581h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F5C50D9257Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F5C50D925C4h
test ah, ah
je 00007F5C50D925B6h
test eax, 00FF0000h
je 00007F5C50D925A5h
test eax, FF000000h
je 00007F5C50D92594h
jmp 00007F5C50D9255Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h

Instruction
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x40b828	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x653000	0x19398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x42c600	0xb80	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x915000	0xddc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	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	0x3150	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40b2ea	0x40b400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x40d000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x653000	0x2c1398	0x19400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x915000	0x5a16	0x5c00	False	0.12958559782608695	data	1.558620115158612	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x653730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x6545d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x654e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x657428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x6584d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x658988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x659830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x65a0d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x65a640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x65cbe8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x65dc90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x65e618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x65eae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x65f990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x660238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x660900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x660e68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x663410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x6644b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x664988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x665830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x6660d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x666640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x668be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x669c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x66a618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x66ad20	0x664	data		
RT_STRING	0x66b388	0x59e	data		
RT_STRING	0x66b928	0x29a	data		
RT_STRING	0x66bbc8	0x248	data		
RT_STRING	0x66be10	0x582	data		
RT_GROUP_ICON	0x66aa80	0x68	data		
RT_GROUP_ICON	0x658938	0x4c	data		
RT_GROUP_ICON	0x664920	0x68	data		
RT_GROUP_ICON	0x65ea80	0x68	data		
RT_VERSION	0x66aae8	0x238	data		

Imports

DLL	Import

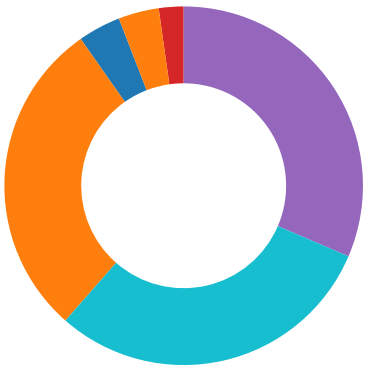
DLL	Import
KERNEL32.dll	GetModuleHandleW, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, AttachConsole, SleepEx, VirtualAlloc, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, GetLongPathNameA, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	GetCharWidthW, EnumFontsW, GetCharABCWidthsFloatW
ADVAPI32.dll	MapGenericMask

Network Behavior

No network behavior found

Statistics

Behavior



- kdsyitkxmS.exe
- powershell.exe
- conhost.exe
- kdsyitkxmS.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- netsh.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: kdsyitkxmS.exe PID: **4652**, Parent PID: **3452**

General

Target ID:	0
Start time:	11:18:56
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\kdsyitkxmS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kdsyitkxmS.exe

Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.374126530.00000000030C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000000.00000002.367355865.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000000.00000003.353503298.00000000039B0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.370479632.0000000002CC1000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000000.00000002.374126530.0000000003503000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000000.00000003.353503298.0000000003DF1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000000.00000002.367355865.0000000000843000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Analysis Process: powershell.exe PID: **5948**, Parent PID: **4652**

General

Target ID:	1
Start time:	11:18:59
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb40000
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\AppData\Local\Temp__PSscriptPolicyTest_zon3rn2d.2u2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p030yzvi.tqg.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
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	7299CF06	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	7299CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B61926	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zon3rn2d.2u2.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p030yzvi.tqg.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zon3rn2d.2u2.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p030yzvi.tqg.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 50 14 00 00 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@eP	success or wait	1	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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 49 00 00 00 0e 00 20 00	H<@^L"My:I	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	255	1	00		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	00 08 00 03		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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 09 06 fd 00 fd 57 40 01 fd 10 40 01 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 00 54 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 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 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 16 3b 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 3b 4d 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 fd 29 40 01 fd 3f 40	T@>@@V@H@X@[@W@@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@Xd@Vd@*@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;@;@;@<@<@;M@<@W@M@D@D@@M@)@?@	success or wait	11	72C676FC	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	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown

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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
stdin	unknown	1024	success or wait	1	717E1B4F	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	717E1B4F	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	717E1B4F	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	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
stdin	unknown	1024	pipe broken	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **5936**, Parent PID: **5948**

General

Target ID:	2
Start time:	11:18:59
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: kdsyitkxmS.exe PID: **3320**, Parent PID: **4652**

General

Target ID:	5
Start time:	11:19:03
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\kdsyitkxmS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kdsyitkxmS.exe
Imagebase:	0x400000
File size:	4379008 bytes
MD5 hash:	01FE6BA28D82175D35665B3EB6ED8CEA
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000005.00000003.368338557.0000000003820000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.622953381.0000000002B35000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000005.00000002.619390815.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000005.00000002.619390815.0000000000843000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000005.00000003.368338557.0000000003C61000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000005.00000002.624452357.0000000003373000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000005.00000002.624452357.0000000002F30000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	88			invalid handle	1	465615	WriteFile
unknown	unknown	605			invalid handle	2	465615	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\kdsyitkxmS.exe	0	96	success or wait	38	465615	ReadFile
C:\Users\user\Desktop\kdsyitkxmS.exe	unknown	4	success or wait	4	465615	ReadFile
\pipe	unknown	512	success or wait	13	465615	ReadFile
\pipe	unknown	1505	pipe broken	1	465615	ReadFile
\pipe	unknown	512	success or wait	2	465615	ReadFile
\pipe	unknown	1017	pipe broken	1	465615	ReadFile
\pipe	unknown	512	success or wait	19	465615	ReadFile
\pipe	unknown	887	pipe broken	1	465615	ReadFile
\pipe	unknown	512	unknown	1	465615	ReadFile

Analysis Process: powershell.exe PID: **7000**, Parent PID: **3320**

General

Target ID:	6
Start time:	11:19:05
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0x7ff745070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
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	71745B28	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	71745B28	unknown
C:\Windows\TEMP__PSscriptPolicyTest_uyxuby1g.134.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Windows\TEMP__PSscriptPolicyTest_1depap5s.43l.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Windows\SysWOW64\config\systemprofile\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	7299CF06	unknown
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B61926	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_uyxuby1g.134.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Windows\Temp__PSscriptPolicyTest_1depap5s.43l.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_uyxuby1g.134.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Windows\Temp__PSscriptPolicyTest_1depap5s.43l.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 4c 14 00 00 19 00 00 00 fd 0d fd 05 35 08 22 08 22 08 00 00 00 00 14 02 34 00 fd 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eL5""4@	success or wait	1	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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 49 00 00 00 0e 00 20 00	H<@^L"My:I	success or wait	17	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	255	1	00		success or wait	11	72C676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	00 08 00 03		success or wait	11	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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 09 0c fd 00 54 01 40 00 fd 3e 40 01 16 3b 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 fd 57 40 01 fd 10 40 01 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 00 54 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 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 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 42 4d 00	T@>@;@@V@H@X@[@W@@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@;@;@<@<@<@W@M@E@!M@;M@D@D@@M@<M@$M@8M@?M@BM	success or wait	11	72C676FC	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	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
stdin	unknown	1024	success or wait	1	717E1B4F	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	717E1B4F	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	717E1B4F	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	717E1B4F	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	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	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	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	717E1B4F	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	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
stdin	unknown	1024	pipe broken	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **7120**, Parent PID: **7000**

General

Target ID:	7
Start time:	11:19:06
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **5952**, Parent PID: **3320**

General

Target ID:	8
Start time:	11:19:10
Start date:	28/05/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes"
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: **5900**, Parent PID: **5952**

General

Target ID:	9
Start time:	11:19:10
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: netsh.exe PID: **2576**, Parent PID: **5952**

General

Target ID:	10
Start time:	11:19:10
Start date:	28/05/2023
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes
Imagebase:	0x7ff762f70000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **2080**, Parent PID: **3320**

General

Target ID:	11
Start time:	11:19:11
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb40000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\TEMP__PScriptPolicyTest_fil3vomk.kwi.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Windows\TEMP__PScriptPolicyTest_mfqj4tng.2eo.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Windows\SysWOW64\config\systemprofile\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	7299CF06	unknown
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PScriptPolicyTest_fil3vomk.kwi.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Windows\Temp__PScriptPolicyTest_mfqj4tng.2eo.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PScriptPolicyTest_fil3vomk.kwi.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Windows\Temp__PScriptPolicyTest_mfqj4tng.2eo.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	1	717E1B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 fd fd fd fd fd fd 12 09 9f fd 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	eInstall-PackageProviderImport-PackageProviderGet-PackageProviderRegister-PackageSourceUninstall-PackageFind-PackageProviderIC:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	12288	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	Resume-BitLockerBackup-BitLockerKeyProtector%Show-BitLockerRequiredActionsInternalUnlock-PasswordInternalUnlock-BitLockerAdd-TpmProtectorInternal%Add-RecoveryPasswordProtectorInternalUnlock-Recover	success or wait	1	717E1B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 4c 14 00 00 19 00 00 00 fd 0d fd 05 35 08 22 08 22 08 00 00 00 00 14 02 34 00 fd 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eL5""4@	success or wait	1	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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 49 00 00 00 0e 00 20 00	H<@^L"My:I	success or wait	17	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	255	1	00		success or wait	11	72C676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	00 08 00 03		success or wait	11	72C676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	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 09 0c fd 00 54 01 40 00 fd 3e 40 01 16 3b 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 fd 57 40 01 fd 10 40 01 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 00 54 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 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 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 42 4d 00	T@>@;@@V@H@X@[@W@@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@;@;@<@<@<@W@M@E@!M@;M@D@D@@M@<M@$M@8M@?M@BM	success or wait	11	72C676FC	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	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
stdin	unknown	1024	success or wait	1	717E1B4F	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	717E1B4F	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	717E1B4F	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	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
stdin	unknown	1024	pipe broken	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **6908**, Parent PID: **2080**

General

Target ID:	12
Start time:	11:19:11
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **4820**, Parent PID: **3320**

General

Target ID:	15
Start time:	11:20:14
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xb40000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile

Analysis Process: conhost.exe PID: **1812**, Parent PID: **4820**

General	
Target ID:	16
Start time:	11:20:14
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly