ID: 234273
Sample Name: CL_Utility.ps1
Cookbook: default.jbs
Time: 18:12:08
Date: 29/05/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

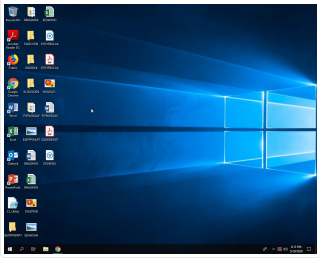
Analysis Report CL_Utility.ps1

Overview

General Information

Sample Name:	CL_Utility.ps1
MD5:	432e8664df006c0.
SHA1:	9072a5f153d5dfd..
SHA256:	5709eadd03ebc2..

Most interesting Screenshot:



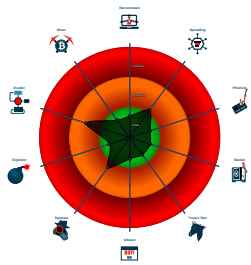
Detection

Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Contains long sleeps (>= 3 min)
- Enables debug privileges
- Found a high number of Window / Us…
- May sleep (evasive loops) to hinder d…
- Queries the volume information (nam…

Classification



Startup

- **System is w10x64**
- powershell.exe (PID: 308 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -noLogo -ExecutionPolicy unrestricted -file 'C:\Users\user\Desktop\CL_Utility.ps1' MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 3740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

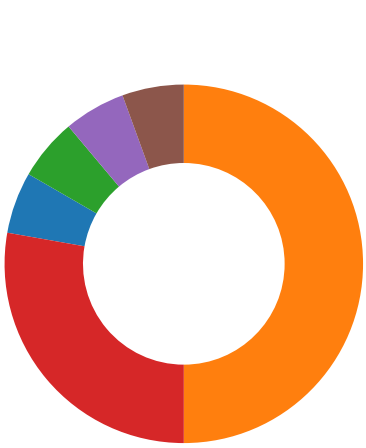
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

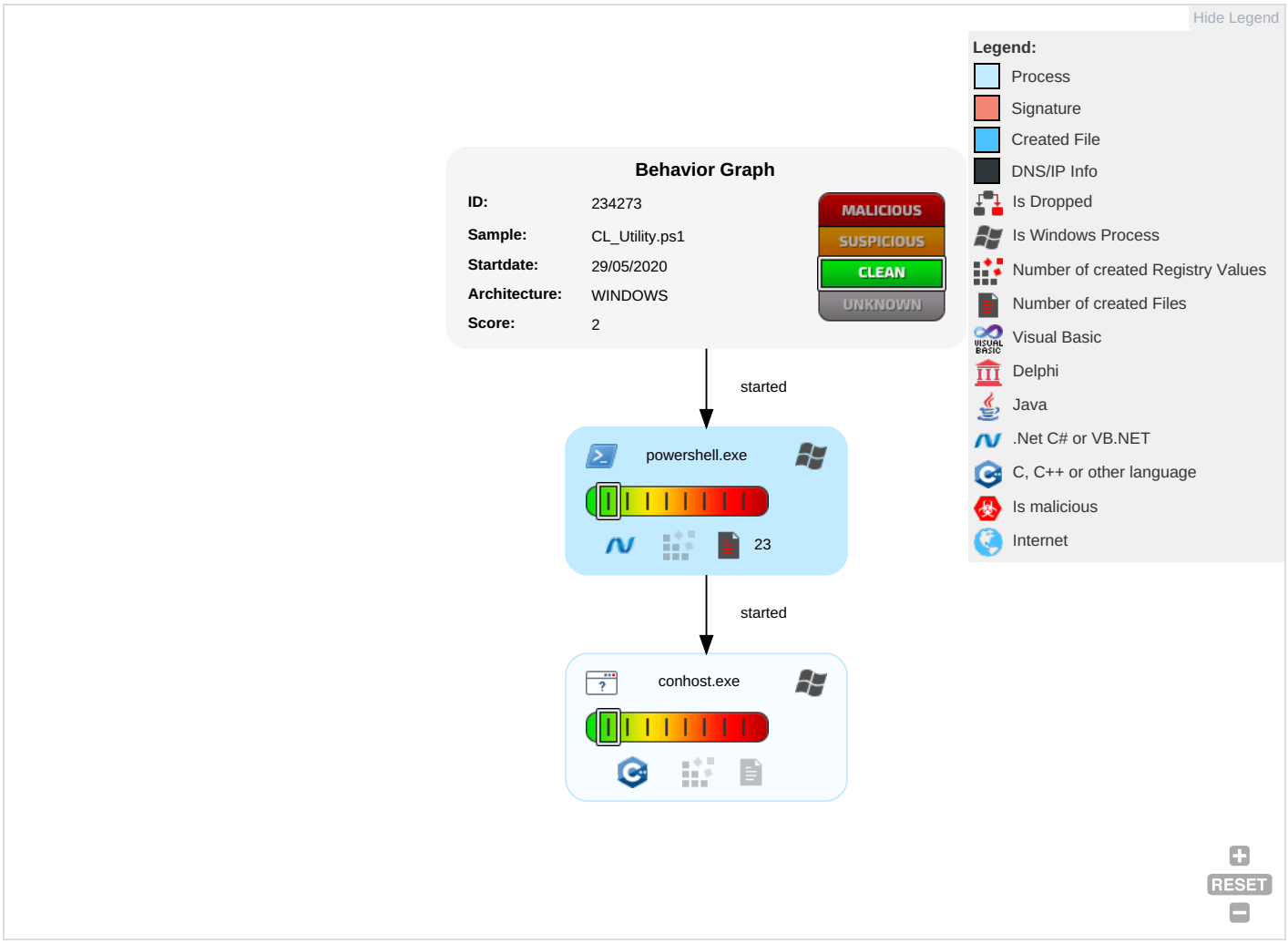


Click to jump to signature section

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Remote Management	Winlogon Helper DLL	Process Injection 1	Masquerading 1	Credential Dumping	Virtualization/Sandbox Evasion 2	Application Deployment Software	Data from Local System	Data Compressed	Data Obfuscation	Eavesdrop o Insecure Network Communicat
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Virtualization/Sandbox Evasion 2	Network Sniffing	Process Discovery 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels	Exploit SS7 t Redirect Pho Calls/SMS
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Process Injection 1	Input Capture	Application Window Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit SS7 t Track Device Location
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information	Credentials in Files	File and Directory Discovery 2	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Card Swap
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Masquerading	Account Manipulation	System Information Discovery 1 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Manipulate Device Communicat

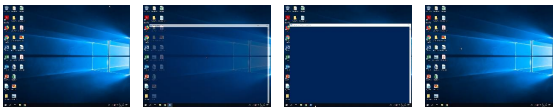
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	234273
Start date:	29.05.2020
Start time:	18:12:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CL_Utility.ps1
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	3
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.winPS1@2/5@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .ps1 • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe

Simulations

Behavior and APIs

Time	Type	Description
18:12:35	API Interceptor	11x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i4cznva5.jvf.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	80
Entropy (8bit):	4.576895309554298
Encrypted:	false
MD5:	9F7768CF6B01D405C945E7A9C001055E
SHA1:	4FA988A735598295C3AF68EFE0BAE7EED15BD34A
SHA-256:	84C81C02C6B1C0F47EBC1967D73069175281FCF6CCBFD754836D400FC6B7C729
SHA-512:	9769FD024DBC6D3EDD52D15A0611347B679493BB4FE0DA2B9F4DFE9206E56FC4C14CAB48E7C7725BF44E19E116D07FE25A3A67AAE22315A4E21FCF210D01055
Malicious:	false
Reputation:	low
Preview:	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 6:12:35 PM

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_noig3sbn.0q4.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	80
Entropy (8bit):	4.576895309554298
Encrypted:	false
MD5:	9F7768CF6B01D405C945E7A9C001055E
SHA1:	4FA988A735598295C3AF68EFE0BAE7EED15BD34A
SHA-256:	84C81C02C6B1C0F47EBC1967D73069175281FCF6CCBFD754836D400FC6B7C729
SHA-512:	9769FD024DBC6D3EDD52D15A0611347B679493BB4FE0DA2B9F4DFE9206E56FC4C14CAB48E7C7725BF44E19E116D07FE25A3A67AAE22315A4E21FCF210D01055
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_noig3sbn.0q4.ps1	
Preview:	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 6:12:35 PM

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\CZ7LSCUDQ5KXFENWP9R3.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Size (bytes):	6206
Entropy (8bit):	3.7001294953253656
Encrypted:	false
MD5:	E1E89B087A3D022C1072C83B2AD675F2
SHA1:	3DB857D79893913AFB6726D5A4757D337B82E7EF
SHA-256:	94B91327A203E7E223804FE2555315C43F7EB663FBA10FB3D6FF9FB45149DDE3
SHA-512:	EC695DB3C7AA055C03A52BB6AB62AC15D2ADC68D5153B1240CB4D5667A0DD29EB3B1BD8AADC8D8101571D8BB9C5E423EE970707D5AF08351C1F6BA28C5AB E9D
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.".. ...YA.....\.....:..DG..Yr?.D..U..k0.&...&.....8Y.....f.6.....t...CFSF..1.....>P...AppData...t.Y^...H.g.3..(... ..gVA.G..k...@.....>P.P.....+.....,...A.p.p.D.a.t.a...B.V.1.....>P...Roaming.@.....>P.P.....]..... R.o.a.m.i.n.g.....\.1.....>P$...MICROS~1..D.....>P.P....._.. .....().M.i.c.r.o.s.o.f.t.....V.1.....>Pu...Windows.@.....>P.>Pu.....a.....q..W.i.n.d.o.w.s.....1.....>P...STARTM~1..n.....>P.>PC.....e.....D.....h...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....Programs..j.....>P.>PC.....g.....@.....g|.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.....>P.>P.....i.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....>P.>P.....

C:\Users\user\Documents\20200529\PowerShell_transcript.830021.lr8aiUAW.20200529181235.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	3979
Entropy (8bit):	5.373795441634861
Encrypted:	false
MD5:	E90DC3C0DC25EFE84C0E7D5BA5F0977F
SHA1:	62C26AE58AA34D92B0AB5E11176115BD7879FCDD
SHA-256:	E70C30B87CCB635753A0CDBA1AC1672C4CAA92482F8667974DDF3EBC41073C38
SHA-512:	67625148C4DE25B29D9F747D8079CA3E98097DCF41EF2E1CCDF859E7233E938B8CC15A4C9A5CBA7266E157BF8A9CC2C95B9E79DDE8D2C4041F2E9577C1C00 A
Malicious:	false
Reputation:	low
Preview:	.**********..Windows PowerShell transcript start..Start time: 20200529181235..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 830021 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noLogo -ExecutionPolicy un restricted -file C:\Users\user\Desktop\CL_Utility.ps1..Process ID: 308..PSVersion: 5.1.17134.165..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.1 7134.165..BuildVersion: 10.0.17134.165..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**** **********..**********..Command start time: 20200529181235..**********..PS>CommandInvocation(CL_Utility.ps1): "CL_Utility.ps1"..********** **********..Windows PowerShell transcript start..Start time: 20200529181236..Username: computer\user..RunAs User: computer\user..Configura

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.0508537093329595
TrID:	
File name:	CL_Utility.ps1
File size:	13799
MD5:	432e8664df006c0a5720fd6ba6759ff6
SHA1:	9072a5f153d5dfd1cfbe54f5a69e8a9a42054f9d
SHA256:	5709eadd03ebc284151b54d86055afcbaafdf38d3f0b9ee 25c321a6749a76089
SHA512:	43c872cf8588efe67dea8d39d90797f6ebb8de379ed71d1 3b3675e467f4e52948b839939bc2e6cf6046b92ed6dbc5a 37cc742e30eb65681c987d9127b88a5a10
SSDEEP:	192:ONIOEyGSWgjRKr5MYnzuQnDjRE+Ol4WWLpLCv FeqNnpUNpSXco6Njip3UvF2fG82:O7I8aaYnyQn/eNb6 NjipEt2vr4r2Y
File Content Preview:	#Common utility functions..Import-LocalizedData -Binding Variable localizationString -FileName CL_Localization Data....# Function to get user troubleshooting history..fu nction Get-UserTSHistoryPath {.. return "${env:locala ppdata}\diagnostics"..}....# Fun

File Icon

Icon Hash:	72f2d6fef6f6dae4

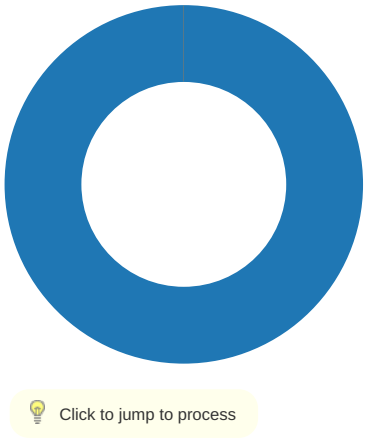
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: powershell.exe PID: 308 Parent PID: 3388

General

Start time:	18:12:33
Start date:	29/05/2020
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\CL_Utility.ps1'
Imagebase:	0x7ff60b9d0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF9E3B4EA15	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	7FF9E3B4EA15	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	7FF9DFAE0A4C	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	7FF9DFAE0A4C	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_noig3sbn.0q4.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF9E2876FFD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_i4cznva5.jvf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF9E2876FFD	CreateFileW
C:\Users\user\Documents\20200529	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF9E287F37D	CreateDirectoryW
C:\Users\user\Documents\20200529\PowerShell_transcript.830021.lr8aiUAW.20200529181235.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF9E2876FFD	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	2	7FF9DFAE0A4C	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	7FF9DFAE0A4C	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	7FF9DFAE0A4C	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	7FF9DFAE0A4C	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	7FF9DFAE0A4C	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	1	7FF9DFAE0A4C	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	7FF9DFAE0A4C	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	7FF9DFAE0A4C	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	7FF9DFAE0A4C	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	7FF9DFAE0A4C	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_noig3sbn.0q4.ps1	success or wait	1	7FF9E287F290	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_i4cznva5.jvf.psm1	success or wait	1	7FF9E287F290	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_noig3sbn.0q4.ps1	unknown	80	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20 35 2f 32 39 2f 32 30 32 30 20 36 3a 31 32 3a 33 35 20 50 4d	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 6:12:35 PM	success or wait	1	7FF9E287B546	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_i4cznva5.jvf.psm1	unknown	80	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20 35 2f 32 39 2f 32 30 32 30 20 36 3a 31 32 3a 33 35 20 50 4d	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 6:12:35 PM	success or wait	1	7FF9E287B546	WriteFile
C:\Users\user\Documents\20200529\PowerShell_transcript.830021.lr8aiUAW.20200529181235.txt	unknown	3	ef bb bf	...	success or wait	1	7FF9E287B546	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20200529\PowerShell_transcript.830021.lr8aiUAW.20200529181235.txt	unknown	689	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 30 35 32 39 31 38 31 32 33 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 53 55 5a 41 4e 4e 45 44 41 56 49 45 53 2d 50 5c 46 61 6c 6c 6f 6e 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 53 55 5a 41 4e 4e 45 44 41 56 49 45 53 2d 50 5c 46 61 6c 6c 6f 6e 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 33 30 30 32 31 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20200529181235..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 830021 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	28	7FF9E287B546	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 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 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FF9E3F6FC88	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	7FF9E3A5C00D	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b818384f6f636b55ba6f5af0c6a7784d\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF9E3A63025	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF9E3A63025	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF9E3A63025	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF9E3A63025	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FF9E3A63025	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	7FF9E3A63025	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FF9E3A63025	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\16f355aec7c0ddbf07e4ba8ea04da1c5\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\ecad7ae388cef8593aaf80bd2e354c40\System.ni.dll.aux	unknown	620	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\c79ff69b8e787a0eab7528231903f272\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\c4851b03ba8d98b41d55d4782c8e58b6\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF9E3A5C00D	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	7FF9E3A5C00D	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF9E3A5C00D	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF9E3A6C9BB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	20448	success or wait	1	7FF9E3A6CA99	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\0 94c2a9cbf04eb358e5edf7e617159de\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\1b 1d43ddf8ad426d8b63cfc742d9fc5e\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\1a9dc87a16846dec37edcec452d3af68\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\c73e2a86060033c34fd87b7cabedb2ae\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\5298d54f2f3b904351a8b2fcd6977f4c\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\fd09ca11fde550312ac2f945d0e1b88d\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\3923669024c3ad21b1f628926196e1af\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e2a9148f660974bf6dd220e59c0c8dfc\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\6c33a9c412951355e66c5772ed21f2ce\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Users\user\Desktop\CL_Utility.ps1	unknown	4096	success or wait	4	7FF9E287B546	ReadFile
C:\Users\user\Desktop\CL_Utility.ps1	unknown	537	end of file	1	7FF9E287B546	ReadFile
C:\Users\user\Desktop\CL_Utility.ps1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF9E287B546	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF9E287B546	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	135	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\93e1697e7e205a939433cd71f5f6f973\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\d4126cede928fd84ab289493035ec27c\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF9E3A16C5B	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	7FF9E287B546	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF9E287B546	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	7FF9E287B546	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	7FF9E287B546	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF9E287B546	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF9E287B546	ReadFile

Analysis Process: conhost.exe PID: 3740 Parent PID: 308

General

Start time:	18:12:34
Start date:	29/05/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b31b0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly