



ID: 829693
Sample Name: script.ps1
Cookbook: default.jbs
Time: 21:39:47
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report script.ps1 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
General Information 7
Warnings 7
Simulations 7
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASNs 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 8
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3lzrlpei.u5a.ps1 8
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xpumcbu2.euy.psm1 9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy) 9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6KV3ER4DHL09F2229XEM.temp 9
Static File Info 10
General 10
File Icon 10
Network Behavior 10
Statistics 10
Behavior 10
System Behavior 11
Analysis Process: powershell.exePID: 5944, Parent PID: 3452 11
General 11
File Activities 11
File Created 11
File Deleted 11
File Written 11
File Read 12
Analysis Process: conhost.exePID: 5932, Parent PID: 5944 13
General 13
Disassembly 13

Copyright Joe Security LLC 2023

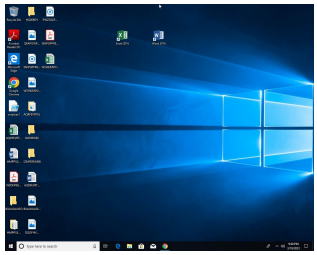
Windows Analysis Report

script.ps1

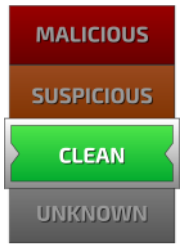
Overview

General Information

Sample Name:	script.ps1
Analysis ID:	829693
MD5:	1b1af89817406..
SHA1:	0eca8e052d8e…
SHA256:	4bb37855cd97…
Infos:	



Detection

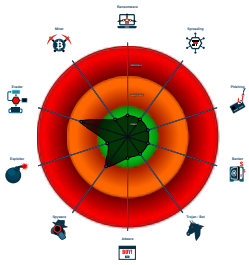


Score:	3
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- powershell.exe (PID: 5944 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noLogo -ExecutionPolicy unrestricted -file "C:\Users\user\Desktop\script.ps1 MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 5932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

Copyright Joe Security LLC 2023

No Snort rule has matched

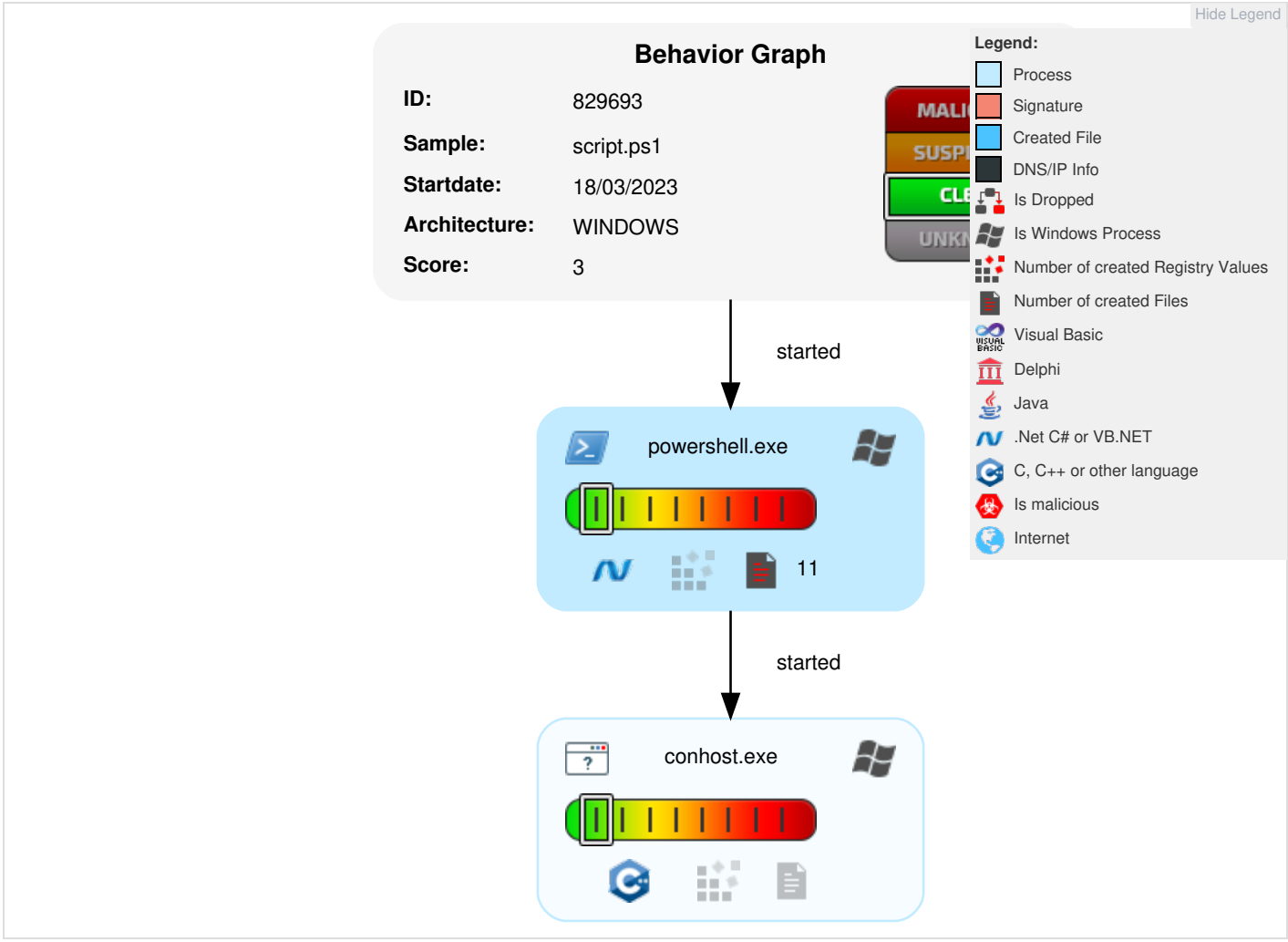
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	Windows Management Instrumentation	Path Interception	1 Process Injection	2 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	2 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 File and Directory 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	Software Packing	LSA Secrets	1 1 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright Joe Security LLC 2023



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

Copyright Joe Security LLC 2023

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000000.00000002.255942686.000002AAB5F81000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829693
Start date and time:	2023-03-18 21:39:47 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 33s
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:	2
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:	script.ps1
Detection:	CLEAN
Classification:	clean3.winPS1@2/5@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .ps1 • Stop behavior analysis, all processes terminated

Warnings

- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Execution Graph export aborted for target powershell.exe, PID 5944 because it is empty
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: script.ps1

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-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_3lzrlpei.u5a.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xpumcbu2.euy.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
Reputation:	high, very likely benign file
Preview:	1

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):	6205
Entropy (8bit):	3.7515618099789605
Encrypted:	false
SSDEEP:	96:InWQFCzQ51DXkvhkvCCtdi5fvDH7L5fvDH7/:lQa4HUVl
MD5:	8A38332F9D8295CC5E991A6879000DE7
SHA1:	06C4B9D34B75C009619E1FFDF9DC057FC6781F22
SHA-256:	41038D6172624501339684F6D025FDC308FB18E5A8D84C09C1D3C5C02E9C2E1F
SHA-512:	E56E1CFAA27A9F6A1AC7F0687A58796C4647F1DD3E3756A9DA276885C2003A1779E854E233A933BD9F2A2A0F5BF2EB5431A79B11C9F3D1A54A909EE90C748177
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-..Z.....R....Z.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny.sV.%.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny.sV.%.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....>QCw..MICROS~1..D.....Ny.sV.%.....Y.....M.i.c.r.o.s.o.f.t.....V.1.....U...Windows.@.....Ny.sV.%.....Y.....W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny.sV.%.....Y.....D.....0.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.q..Programs..j.....Ny.sV.%.....Y.....@.....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.....Ny..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..^.....Ny..P.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6KV3ER4DHL09F2229XEM.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6205
Entropy (8bit):	3.7515618099789605
Encrypted:	false
SSDEEP:	96:InWQFCzQ51DXkvhkvCCtdi5fvDH7L5fvDH7/:lQa4HUVl
MD5:	8A38332F9D8295CC5E991A6879000DE7
SHA1:	06C4B9D34B75C009619E1FFDF9DC057FC6781F22
SHA-256:	41038D6172624501339684F6D025FDC308FB18E5A8D84C09C1D3C5C02E9C2E1F
SHA-512:	E56E1CFAA27A9F6A1AC7F0687A58796C4647F1DD3E3756A9DA276885C2003A1779E854E233A933BD9F2A2A0F5BF2EB5431A79B11C9F3D1A54A909EE90C748177
Malicious:	false

Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-..Z.....R....Z.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny.sV.%.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny.sV.%.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....>QCw..MICROS~1..D.....Ny.sV.%.....Y.....M.i.c.r.o.s.o.f.t.....V.1.....U...Windows.@.....Ny.sV.%.....Y.....W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny.sV.%.....Y.....D.....0.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.q..Programs..j.....Ny.sV.%.....Y.....@.....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.....Ny..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..^.....Ny..P.....Y.....

Static File Info

General

File type:	Unicode text, UTF-8 text, with very long lines (11724)
Entropy (8bit):	3.5009067194017636
TrID:	
File name:	script.ps1
File size:	12257
MD5:	1b1af8981740660f00051bdd98caed74
SHA1:	0eca8e052d8eadcdf0d331144289be9395bc2cee
SHA256:	4bb37855cd9767eb6fd77e1324c35187121eeef26c265166cbc15e458563eb7a
SHA512:	1312ce00bde457dfdf6d6a8a2cafea719b411571355f374c76c862f6e2240ee1bfca75db0640cdff3421987317da7fc27cb5e9a05658c6652d88eb4f8e482a2c
SSDEEP:	96:APCNIAnOsqooAwAAAAwAAAAAAwAwAAwwAAwAAwwAAADAxooAAAwAAAAwAIAAAAAc:Pur
TLSH:	144236C1E5CAD7B0D42605521C51767B23DE6BE79A8B20F6FF866EFF94E4172080B824
File Content Preview:	${[~@} = $(); ${!!@!!]} = ++${[~@}; ${[[!} = --${[~@} + ${!!@!!]} + ${!!@!!]}; ${~~~]} = ${[[!} + ${!!@!!]}; ${[!!![!} = ${[[!} + ${[[!}; ${(~(!} = ${~~~]} + ${[[!}; ${!~!))} = ${[!!![!} + ${[[!}; ${(((!} = ${!!@!!]} + ${[!!![!} + ${[[!}; ${=!!@!!} ..= ${~~~]

File Icon



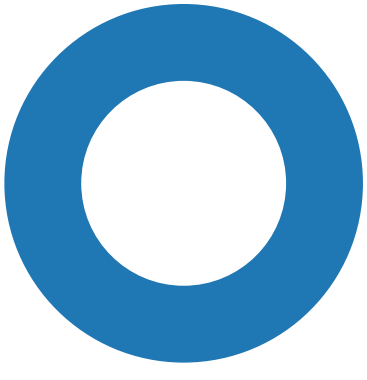
Icon Hash:	72f2d6fef6f6dae4

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: powershell.exe PID: **5944**, Parent PID: **3452**

General

Target ID:	0
Start time:	21:40:41
Start date:	18/03/2023
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\script.ps1
Imagebase:	0x7ff65fab0000
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	7FFC08AA03FC	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	7FFC08AA03FC	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_3lzrlpei.u5a.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_xpumcbu2.euy.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B786FDD	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	7FFC0CA5F1E9	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	7FFC0CA5F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_3lzrlpei.u5a.ps1	success or wait	1	7FFC0B78F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_xpumcbu2.euy.psm1	success or wait	1	7FFC0B78F270	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__PScriptPolicyTest_3lzrlpei.u5a.ps1	0	1	31	1	success or wait	1	7FFC0B78B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xpumcbu2.euy.psm1	0	1	31	1	success or wait	1	7FFC0B78B526	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 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	7FFC0CE7F6E8	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	7FFC0C92B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0C92B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C92B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0C92B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0C932625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0C932625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C932625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0C92B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0C92B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0C92B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0C92B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0CA012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0C9162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7FFC0C9163B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0CA012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0CA012E7	ReadFile
C:\Users\user\Desktop\script.ps1	unknown	4096	success or wait	3	7FFC0B78B526	ReadFile
C:\Users\user\Desktop\script.ps1	unknown	31	end of file	1	7FFC0B78B526	ReadFile
C:\Users\user\Desktop\script.ps1	unknown	4096	end of file	1	7FFC0B78B526	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	7FFC0C92B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0C92B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC0B78B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC0B78B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC0B78B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC0B78B526	ReadFile

Analysis Process: conhost.exe PID: **5932**, Parent PID: **5944**

General

Target ID:	1
Start time:	21:40:41
Start date:	18/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly