ID: 1579432
Sample Name: 3.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:52:37
Date: 22/12/2024
Version: 41.0.0 Charoite

Table of Contents

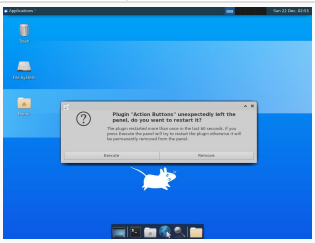
Linux Analysis Report

3.elf

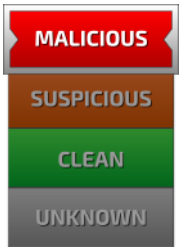
Overview

General Information

Sample name:	3.elf
Analysis ID:	1579432
MD5:	4063c4d9a590…
SHA1:	0a80aa5fb17e2..
SHA256:	909e64490c57…
Tags:	elf user-abuse_ch
Infos:	



Detection

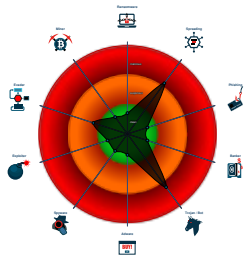


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Suricata IDS alerts for network traffic
- Connects to many ports of the same…
- Sample tries to kill multiple process…
- Uses known network protocols on n…
- Detected TCP or UDP traffic on non…
- Detected non-DNS traffic on DNS po…
- Enumerates processes within the "p…
- HTTP GET or POST without a user …
- Sample contains strings indicative o…

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1579432
Start date and time:	2024-12-22 09:52:37 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Sample name:	3.elf
Detection:	MAL
Classification:	mal76.spre.troj.linELF@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/3.elf
PID:	5558
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	gosh that chinese family at the other table sure ate a lot
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 3.elf (PID: 5558, Parent: 5475, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/3.elf
  - 3.elf New Fork (PID: 5566, Parent: 5558)
    - 3.elf New Fork (PID: 5568, Parent: 5566)
      - 3.elf New Fork (PID: 5572, Parent: 5568)
      - 3.elf New Fork (PID: 5573, Parent: 5568)
      - 3.elf New Fork (PID: 5576, Parent: 5568)
- xfce4-panel New Fork (PID: 5560, Parent: 3172)
- wrapper-2.0 (PID: 5560, Parent: 3172, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 6 12582920 systray "Notification Area" "Area where notification icons appear"
- xfce4-panel New Fork (PID: 5561, Parent: 3172)
- wrapper-2.0 (PID: 5561, Parent: 3172, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libstatusnotifier.so 7 12582921 statusnotifier "Status Notifier Plugin" "Provides a panel area for status notifier items (application indicators)"
- xfce4-panel New Fork (PID: 5562, Parent: 3172)
- wrapper-2.0 (PID: 5562, Parent: 3172, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 8 12582922 pulseaudio "PulseAudio Plugin" "Adjust the audio volume of the PulseAudio sound system"
- xfce4-panel New Fork (PID: 5563, Parent: 3172)
- wrapper-2.0 (PID: 5563, Parent: 3172, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 9 12582923 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
- xfce4-panel New Fork (PID: 5564, Parent: 3172)
- wrapper-2.0 (PID: 5564, Parent: 3172, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
- xfce4-panel New Fork (PID: 5565, Parent: 3172)
- wrapper-2.0 (PID: 5565, Parent: 3172, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 14 12582925 actions "Action Buttons" "Log out, lock or other system actions"
- **cleanup**

Yara Signatures

No yara matches

Suricata Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:09.198274+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41138	197.8.44.33	37215	TCP
2024-12-22T09:54:09.424133+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52976	197.234.184.83	37215	TCP
2024-12-22T09:54:09.693632+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34668	41.175.153.229	37215	TCP
2024-12-22T09:54:12.049891+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54032	192.158.238.237	37215	TCP
2024-12-22T09:54:12.508554+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56430	157.70.215.31	37215	TCP
2024-12-22T09:54:13.530670+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36286	157.25.23.73	37215	TCP
2024-12-22T09:54:14.409934+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58222	94.121.205.148	37215	TCP
2024-12-22T09:54:15.144818+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59856	216.172.184.107	37215	TCP
2024-12-22T09:54:15.598336+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41874	58.125.17.184	37215	TCP
2024-12-22T09:54:15.892277+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56240	197.79.1.153	37215	TCP
2024-12-22T09:54:15.893158+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53936	41.160.23.82	37215	TCP
2024-12-22T09:54:16.667405+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35422	190.111.217.223	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:17.024085+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33734	197.130.103.71	37215	TCP
2024-12-22T09:54:18.647997+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40298	69.55.194.147	37215	TCP
2024-12-22T09:54:19.166930+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48684	103.196.161.173	37215	TCP
2024-12-22T09:54:19.215035+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41512	41.175.103.46	37215	TCP
2024-12-22T09:54:19.241976+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37746	27.7.50.15	37215	TCP
2024-12-22T09:54:19.531696+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58328	197.131.155.200	37215	TCP
2024-12-22T09:54:21.548851+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38556	197.96.88.66	37215	TCP
2024-12-22T09:54:23.465525+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53024	197.130.95.95	37215	TCP
2024-12-22T09:54:24.452706+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46964	157.15.182.30	37215	TCP
2024-12-22T09:54:24.644617+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51724	197.8.125.67	37215	TCP
2024-12-22T09:54:25.428788+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52900	126.55.210.116	37215	TCP
2024-12-22T09:54:25.467008+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59018	126.77.245.205	37215	TCP
2024-12-22T09:54:25.588143+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44832	41.180.59.65	37215	TCP
2024-12-22T09:54:26.359484+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43078	157.97.92.217	37215	TCP
2024-12-22T09:54:26.468614+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33524	157.212.222.149	37215	TCP
2024-12-22T09:54:26.468707+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59662	164.68.151.57	37215	TCP
2024-12-22T09:54:26.468858+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56400	116.253.138.61	37215	TCP
2024-12-22T09:54:26.484259+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53612	41.130.58.215	37215	TCP
2024-12-22T09:54:26.484395+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58442	157.97.136.251	37215	TCP
2024-12-22T09:54:26.484492+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53198	41.23.130.146	37215	TCP
2024-12-22T09:54:26.484660+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43484	157.117.78.8	37215	TCP
2024-12-22T09:54:26.484698+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47192	157.198.199.199	37215	TCP
2024-12-22T09:54:26.484820+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42714	41.16.101.255	37215	TCP
2024-12-22T09:54:26.484916+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49520	148.125.168.63	37215	TCP
2024-12-22T09:54:26.485128+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38284	159.95.198.35	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:26.485148+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51124	157.8.141.176	37215	TCP
2024-12-22T09:54:26.485316+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57594	41.9.170.4	37215	TCP
2024-12-22T09:54:26.485451+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51990	157.240.23.156	37215	TCP
2024-12-22T09:54:26.485512+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33576	210.147.121.17	37215	TCP
2024-12-22T09:54:26.485617+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51190	130.223.41.152	37215	TCP
2024-12-22T09:54:26.485681+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34962	197.201.114.176	37215	TCP
2024-12-22T09:54:26.485828+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46698	197.236.36.156	37215	TCP
2024-12-22T09:54:26.485947+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50116	41.147.22.216	37215	TCP
2024-12-22T09:54:26.486032+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56216	41.36.58.35	37215	TCP
2024-12-22T09:54:26.486197+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59296	157.155.234.87	37215	TCP
2024-12-22T09:54:26.486467+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55494	74.177.63.156	37215	TCP
2024-12-22T09:54:26.499760+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38822	143.93.223.56	37215	TCP
2024-12-22T09:54:26.499850+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47276	41.136.164.85	37215	TCP
2024-12-22T09:54:26.499886+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51860	41.119.52.109	37215	TCP
2024-12-22T09:54:26.515575+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40556	41.134.226.53	37215	TCP
2024-12-22T09:54:26.515671+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39404	197.105.18.62	37215	TCP
2024-12-22T09:54:26.515681+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52286	197.79.252.108	37215	TCP
2024-12-22T09:54:26.562577+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49730	41.5.185.41	37215	TCP
2024-12-22T09:54:26.562611+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43662	197.123.70.200	37215	TCP
2024-12-22T09:54:26.562678+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36492	104.184.158.66	37215	TCP
2024-12-22T09:54:26.804303+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44470	222.145.114.194	37215	TCP
2024-12-22T09:54:27.249688+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56528	157.108.252.165	37215	TCP
2024-12-22T09:54:27.265280+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54616	41.183.31.203	37215	TCP
2024-12-22T09:54:27.265382+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37300	157.51.247.114	37215	TCP
2024-12-22T09:54:27.265567+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50552	195.218.231.50	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:27.281007+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51102	41.157.137.219	37215	TCP
2024-12-22T09:54:27.281089+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50080	157.58.177.30	37215	TCP
2024-12-22T09:54:27.281179+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36758	197.39.181.173	37215	TCP
2024-12-22T09:54:27.284992+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39470	157.90.244.87	37215	TCP
2024-12-22T09:54:27.296595+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42430	41.181.52.151	37215	TCP
2024-12-22T09:54:27.296719+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43932	197.154.0.129	37215	TCP
2024-12-22T09:54:27.296803+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46382	197.60.78.44	37215	TCP
2024-12-22T09:54:27.296919+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49888	41.186.240.129	37215	TCP
2024-12-22T09:54:27.297062+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38582	197.214.187.242	37215	TCP
2024-12-22T09:54:27.297191+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39996	197.142.123.239	37215	TCP
2024-12-22T09:54:27.515348+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41764	41.148.226.129	37215	TCP
2024-12-22T09:54:27.515475+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39870	157.87.159.28	37215	TCP
2024-12-22T09:54:27.515538+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51764	157.97.73.39	37215	TCP
2024-12-22T09:54:27.515603+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33868	157.47.242.235	37215	TCP
2024-12-22T09:54:27.515718+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57778	193.254.103.145	37215	TCP
2024-12-22T09:54:27.515824+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53248	41.20.137.108	37215	TCP
2024-12-22T09:54:27.530880+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38358	197.88.175.54	37215	TCP
2024-12-22T09:54:27.531040+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40840	41.205.6.37	37215	TCP
2024-12-22T09:54:27.531080+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43546	197.200.93.131	37215	TCP
2024-12-22T09:54:27.531182+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51288	41.76.174.231	37215	TCP
2024-12-22T09:54:27.531286+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55108	157.187.30.13	37215	TCP
2024-12-22T09:54:27.531445+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58572	41.208.156.218	37215	TCP
2024-12-22T09:54:27.531487+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37052	157.181.120.184	37215	TCP
2024-12-22T09:54:27.546921+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56626	157.53.229.73	37215	TCP
2024-12-22T09:54:27.562397+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47908	157.24.149.224	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:27.562406+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40498	197.137.175.56	37215	TCP
2024-12-22T09:54:27.577897+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46468	197.106.58.1	37215	TCP
2024-12-22T09:54:27.594280+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52028	41.67.7.71	37215	TCP
2024-12-22T09:54:27.609341+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47694	197.39.211.11	37215	TCP
2024-12-22T09:54:27.625012+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53048	157.205.43.230	37215	TCP
2024-12-22T09:54:27.640434+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48660	157.206.148.101	37215	TCP
2024-12-22T09:54:27.640536+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37286	157.20.144.151	37215	TCP
2024-12-22T09:54:27.640694+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39788	197.96.37.76	37215	TCP
2024-12-22T09:54:27.656122+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43910	41.81.4.100	37215	TCP
2024-12-22T09:54:27.656244+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41746	197.45.32.190	37215	TCP
2024-12-22T09:54:27.656430+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48762	157.127.74.230	37215	TCP
2024-12-22T09:54:27.656567+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38284	197.208.96.236	37215	TCP
2024-12-22T09:54:27.671649+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35826	157.214.180.28	37215	TCP
2024-12-22T09:54:27.687392+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51684	197.103.59.243	37215	TCP
2024-12-22T09:54:27.687449+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34216	157.61.126.107	37215	TCP
2024-12-22T09:54:27.760185+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38310	41.175.14.253	37215	TCP
2024-12-22T09:54:28.656454+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58064	41.150.101.178	37215	TCP
2024-12-22T09:54:28.671846+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33554	157.177.163.177	37215	TCP
2024-12-22T09:54:28.671866+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33654	222.56.33.107	37215	TCP
2024-12-22T09:54:28.672018+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55362	197.84.170.215	37215	TCP
2024-12-22T09:54:28.672111+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45852	157.18.29.81	37215	TCP
2024-12-22T09:54:28.672254+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40980	41.104.210.63	37215	TCP
2024-12-22T09:54:28.672334+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37734	47.150.218.100	37215	TCP
2024-12-22T09:54:28.672362+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52354	197.26.203.165	37215	TCP
2024-12-22T09:54:28.687414+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35774	41.86.192.23	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:28.687531+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39266	41.39.157.52	37215	TCP
2024-12-22T09:54:28.687621+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38804	75.215.82.126	37215	TCP
2024-12-22T09:54:28.687766+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37810	91.244.234.3	37215	TCP
2024-12-22T09:54:28.687895+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44282	186.2.18.215	37215	TCP
2024-12-22T09:54:28.687993+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44468	75.161.123.10	37215	TCP
2024-12-22T09:54:28.688167+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42888	157.76.79.65	37215	TCP
2024-12-22T09:54:28.688297+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51804	157.96.157.112	37215	TCP
2024-12-22T09:54:28.688509+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48012	183.180.168.157	37215	TCP
2024-12-22T09:54:28.688681+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41056	41.35.181.9	37215	TCP
2024-12-22T09:54:28.688815+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48120	41.229.147.16	37215	TCP
2024-12-22T09:54:28.688880+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39148	41.137.74.188	37215	TCP
2024-12-22T09:54:28.689045+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57532	41.129.24.92	37215	TCP
2024-12-22T09:54:28.689178+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44172	157.71.136.134	37215	TCP
2024-12-22T09:54:28.689297+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59784	157.22.61.101	37215	TCP
2024-12-22T09:54:28.689383+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50216	197.162.97.194	37215	TCP
2024-12-22T09:54:28.689482+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60148	41.13.114.85	37215	TCP
2024-12-22T09:54:28.689571+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41462	157.86.245.102	37215	TCP
2024-12-22T09:54:28.689773+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43182	157.29.49.0	37215	TCP
2024-12-22T09:54:28.689903+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58958	183.218.229.124	37215	TCP
2024-12-22T09:54:28.690024+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49738	197.28.6.169	37215	TCP
2024-12-22T09:54:28.690103+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58866	81.216.206.52	37215	TCP
2024-12-22T09:54:28.690334+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50870	101.177.12.75	37215	TCP
2024-12-22T09:54:28.690468+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54784	143.92.250.1	37215	TCP
2024-12-22T09:54:28.690550+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45934	160.52.86.56	37215	TCP
2024-12-22T09:54:28.690709+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52708	197.126.129.166	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:28.718616+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57478	189.183.109.113	37215	TCP
2024-12-22T09:54:28.718710+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53274	41.216.98.247	37215	TCP
2024-12-22T09:54:28.718844+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51258	197.68.125.160	37215	TCP
2024-12-22T09:54:28.718971+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51622	203.7.240.130	37215	TCP
2024-12-22T09:54:28.719110+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41486	197.190.246.243	37215	TCP
2024-12-22T09:54:28.719233+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41946	130.194.13.32	37215	TCP
2024-12-22T09:54:28.719391+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39568	43.71.255.139	37215	TCP
2024-12-22T09:54:28.719471+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42154	157.207.215.253	37215	TCP
2024-12-22T09:54:28.719539+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46432	41.26.89.205	37215	TCP
2024-12-22T09:54:28.719735+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33636	57.31.9.67	37215	TCP
2024-12-22T09:54:28.796638+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48992	157.87.198.107	37215	TCP
2024-12-22T09:54:28.803435+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44106	197.181.105.208	37215	TCP
2024-12-22T09:54:28.803593+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58306	197.177.131.26	37215	TCP
2024-12-22T09:54:28.812185+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41806	41.208.1.52	37215	TCP
2024-12-22T09:54:28.812348+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53082	197.204.163.228	37215	TCP
2024-12-22T09:54:28.812482+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35452	41.1.52.53	37215	TCP
2024-12-22T09:54:28.812651+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49722	157.227.220.23	37215	TCP
2024-12-22T09:54:28.812761+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42718	180.46.37.61	37215	TCP
2024-12-22T09:54:28.812898+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33738	197.25.193.152	37215	TCP
2024-12-22T09:54:28.813061+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44080	197.20.125.221	37215	TCP
2024-12-22T09:54:28.813285+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45824	157.78.246.143	37215	TCP
2024-12-22T09:54:28.813404+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50000	157.6.135.22	37215	TCP
2024-12-22T09:54:28.813522+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40112	197.108.155.249	37215	TCP
2024-12-22T09:54:29.531244+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41616	41.140.24.85	37215	TCP
2024-12-22T09:54:29.531460+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59000	195.227.69.17	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:29.531556+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44370	41.86.110.125	37215	TCP
2024-12-22T09:54:29.531634+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46438	41.164.5.41	37215	TCP
2024-12-22T09:54:29.546900+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36414	197.209.246.114	37215	TCP
2024-12-22T09:54:29.547009+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33652	20.87.214.216	37215	TCP
2024-12-22T09:54:29.547100+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39410	41.118.44.139	37215	TCP
2024-12-22T09:54:29.547162+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47780	168.226.133.129	37215	TCP
2024-12-22T09:54:29.562396+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60388	184.244.251.232	37215	TCP
2024-12-22T09:54:29.562522+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55328	41.242.233.42	37215	TCP
2024-12-22T09:54:29.562649+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50104	157.121.228.177	37215	TCP
2024-12-22T09:54:29.562672+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57802	197.25.158.160	37215	TCP
2024-12-22T09:54:29.562833+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50140	81.191.160.152	37215	TCP
2024-12-22T09:54:29.562884+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60824	157.154.202.117	37215	TCP
2024-12-22T09:54:29.563090+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44990	41.45.211.90	37215	TCP
2024-12-22T09:54:29.563186+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56576	41.252.119.148	37215	TCP
2024-12-22T09:54:29.563392+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58454	157.26.100.2	37215	TCP
2024-12-22T09:54:29.563494+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41492	197.9.32.122	37215	TCP
2024-12-22T09:54:29.563641+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51436	52.220.227.249	37215	TCP
2024-12-22T09:54:29.577984+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53904	197.239.140.210	37215	TCP
2024-12-22T09:54:29.578146+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53458	75.190.174.103	37215	TCP
2024-12-22T09:54:29.578176+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53442	197.223.10.64	37215	TCP
2024-12-22T09:54:29.578382+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33274	41.224.49.149	37215	TCP
2024-12-22T09:54:29.578488+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59672	41.143.89.233	37215	TCP
2024-12-22T09:54:29.578582+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37694	41.237.42.179	37215	TCP
2024-12-22T09:54:29.578726+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39808	89.76.195.178	37215	TCP
2024-12-22T09:54:29.578824+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56808	107.58.133.196	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:29.578972+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43310	65.213.58.156	37215	TCP
2024-12-22T09:54:29.579271+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36278	43.92.198.168	37215	TCP
2024-12-22T09:54:29.579456+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44468	157.90.220.190	37215	TCP
2024-12-22T09:54:29.579557+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45278	41.50.182.238	37215	TCP
2024-12-22T09:54:29.579716+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47496	20.0.88.186	37215	TCP
2024-12-22T09:54:29.579876+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47266	93.233.231.169	37215	TCP
2024-12-22T09:54:29.580026+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41616	197.206.51.156	37215	TCP
2024-12-22T09:54:29.580139+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39282	116.0.252.48	37215	TCP
2024-12-22T09:54:29.580304+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57974	157.93.31.153	37215	TCP
2024-12-22T09:54:29.580431+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57254	157.145.4.173	37215	TCP
2024-12-22T09:54:29.580549+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40574	41.98.245.14	37215	TCP
2024-12-22T09:54:29.580585+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34448	157.35.55.24	37215	TCP
2024-12-22T09:54:29.593506+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51096	41.26.23.169	37215	TCP
2024-12-22T09:54:29.593635+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56134	157.239.244.189	37215	TCP
2024-12-22T09:54:29.593743+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33286	157.208.40.95	37215	TCP
2024-12-22T09:54:29.593920+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39406	197.85.171.173	37215	TCP
2024-12-22T09:54:29.594045+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58590	157.214.105.119	37215	TCP
2024-12-22T09:54:29.594184+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49812	197.223.203.65	37215	TCP
2024-12-22T09:54:29.594302+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37464	157.242.148.55	37215	TCP
2024-12-22T09:54:29.594554+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43080	76.112.145.202	37215	TCP
2024-12-22T09:54:29.594598+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60716	197.211.128.1	37215	TCP
2024-12-22T09:54:29.594720+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52196	53.204.222.67	37215	TCP
2024-12-22T09:54:29.640511+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36534	197.240.71.169	37215	TCP
2024-12-22T09:54:29.687671+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34314	197.182.114.58	37215	TCP
2024-12-22T09:54:29.703116+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33148	41.139.238.45	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:29.703241+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57692	41.242.29.160	37215	TCP
2024-12-22T09:54:29.781309+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59678	157.222.40.29	37215	TCP
2024-12-22T09:54:29.796611+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52646	122.251.144.61	37215	TCP
2024-12-22T09:54:29.796691+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41678	41.203.136.73	37215	TCP
2024-12-22T09:54:29.812639+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35826	197.67.145.250	37215	TCP
2024-12-22T09:54:29.812692+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58084	157.212.245.162	37215	TCP
2024-12-22T09:54:29.812846+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55200	41.69.126.24	37215	TCP
2024-12-22T09:54:29.812918+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32768	41.13.58.48	37215	TCP
2024-12-22T09:54:29.813002+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36324	41.99.200.127	37215	TCP
2024-12-22T09:54:29.813111+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34536	197.52.102.205	37215	TCP
2024-12-22T09:54:29.813273+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41802	157.93.20.165	37215	TCP
2024-12-22T09:54:29.813403+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53648	41.128.81.128	37215	TCP
2024-12-22T09:54:29.828060+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53744	157.2.95.174	37215	TCP
2024-12-22T09:54:30.587239+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36432	157.161.255.5	37215	TCP
2024-12-22T09:54:30.687355+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54006	157.118.148.134	37215	TCP
2024-12-22T09:54:30.687531+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58292	84.64.32.109	37215	TCP
2024-12-22T09:54:30.687647+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42320	157.97.24.174	37215	TCP
2024-12-22T09:54:30.687762+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56294	157.40.208.249	37215	TCP
2024-12-22T09:54:30.687922+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57180	197.44.131.108	37215	TCP
2024-12-22T09:54:30.688085+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45338	41.249.54.244	37215	TCP
2024-12-22T09:54:30.688208+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34004	143.229.146.137	37215	TCP
2024-12-22T09:54:30.688329+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59036	41.33.229.30	37215	TCP
2024-12-22T09:54:30.688432+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60140	41.85.52.93	37215	TCP
2024-12-22T09:54:30.688562+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45392	157.204.104.209	37215	TCP
2024-12-22T09:54:30.688785+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51416	197.233.151.209	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:30.688887+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40412	197.190.120.144	37215	TCP
2024-12-22T09:54:30.688985+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53996	197.202.20.213	37215	TCP
2024-12-22T09:54:30.689164+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48004	157.169.78.81	37215	TCP
2024-12-22T09:54:30.689427+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56508	197.98.73.12	37215	TCP
2024-12-22T09:54:30.689542+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37298	41.88.234.15	37215	TCP
2024-12-22T09:54:30.689643+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38932	88.82.33.192	37215	TCP
2024-12-22T09:54:30.689789+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59402	197.182.144.123	37215	TCP
2024-12-22T09:54:30.689912+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50058	163.226.218.0	37215	TCP
2024-12-22T09:54:30.690013+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43848	143.158.252.131	37215	TCP
2024-12-22T09:54:30.690122+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41368	197.38.250.83	37215	TCP
2024-12-22T09:54:30.690254+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56498	197.183.57.234	37215	TCP
2024-12-22T09:54:30.690365+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47434	157.58.173.13	37215	TCP
2024-12-22T09:54:30.690498+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43176	157.120.146.98	37215	TCP
2024-12-22T09:54:30.690608+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60354	157.151.3.153	37215	TCP
2024-12-22T09:54:30.690737+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52748	189.93.52.121	37215	TCP
2024-12-22T09:54:30.690851+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40594	168.180.70.181	37215	TCP
2024-12-22T09:54:30.690933+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40446	138.239.183.100	37215	TCP
2024-12-22T09:54:30.691035+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37660	41.9.165.26	37215	TCP
2024-12-22T09:54:30.691155+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40848	157.169.35.141	37215	TCP
2024-12-22T09:54:30.691346+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53346	140.181.132.148	37215	TCP
2024-12-22T09:54:30.691496+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43524	197.166.126.43	37215	TCP
2024-12-22T09:54:30.691661+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35388	157.69.32.146	37215	TCP
2024-12-22T09:54:30.691927+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45318	209.178.86.248	37215	TCP
2024-12-22T09:54:30.692088+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45386	90.233.74.9	37215	TCP
2024-12-22T09:54:30.692292+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52372	41.133.219.10	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:30.718622+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60842	77.118.183.164	37215	TCP
2024-12-22T09:54:30.725521+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45406	41.47.186.85	37215	TCP
2024-12-22T09:54:30.734338+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58566	197.58.78.221	37215	TCP
2024-12-22T09:54:30.734409+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44084	197.175.159.24	37215	TCP
2024-12-22T09:54:30.734437+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55952	80.9.142.201	37215	TCP
2024-12-22T09:54:30.734530+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51776	41.125.231.243	37215	TCP
2024-12-22T09:54:30.734566+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42412	197.228.1.0	37215	TCP
2024-12-22T09:54:30.734671+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58556	197.242.32.201	37215	TCP
2024-12-22T09:54:30.734781+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53816	197.152.156.114	37215	TCP
2024-12-22T09:54:30.828469+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47394	41.234.174.75	37215	TCP
2024-12-22T09:54:30.828469+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35472	157.63.231.146	37215	TCP
2024-12-22T09:54:30.828478+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48166	197.77.93.138	37215	TCP
2024-12-22T09:54:30.914370+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51882	197.215.218.231	37215	TCP
2024-12-22T09:54:31.859373+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52930	157.244.148.110	37215	TCP
2024-12-22T09:54:31.859431+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41762	60.180.176.199	37215	TCP
2024-12-22T09:54:31.859478+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58856	17.18.223.255	37215	TCP
2024-12-22T09:54:31.984473+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51492	187.94.63.249	37215	TCP
2024-12-22T09:54:31.984499+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38688	41.151.220.159	37215	TCP
2024-12-22T09:54:31.990847+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57510	41.41.203.128	37215	TCP
2024-12-22T09:54:31.990889+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55622	197.155.35.161	37215	TCP
2024-12-22T09:54:31.990905+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34978	197.173.55.207	37215	TCP
2024-12-22T09:54:31.991013+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33094	157.148.167.181	37215	TCP
2024-12-22T09:54:31.991103+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55162	41.59.216.125	37215	TCP
2024-12-22T09:54:31.991227+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49834	95.255.215.200	37215	TCP
2024-12-22T09:54:31.991403+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42394	116.86.106.134	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:31.991495+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55826	197.34.99.195	37215	TCP
2024-12-22T09:54:32.021627+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56946	157.250.111.37	37215	TCP
2024-12-22T09:54:32.021663+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58632	157.27.171.67	37215	TCP
2024-12-22T09:54:32.032812+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36776	197.41.197.99	37215	TCP
2024-12-22T09:54:32.828265+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46016	36.72.0.118	37215	TCP
2024-12-22T09:54:32.843770+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55392	54.97.133.72	37215	TCP
2024-12-22T09:54:32.843969+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39180	197.46.45.137	37215	TCP
2024-12-22T09:54:32.843969+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46014	41.2.218.69	37215	TCP
2024-12-22T09:54:32.843973+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53174	197.162.33.29	37215	TCP
2024-12-22T09:54:32.844068+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34862	157.148.224.133	37215	TCP
2024-12-22T09:54:32.844287+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37678	73.55.9.63	37215	TCP
2024-12-22T09:54:32.844366+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56056	197.28.96.46	37215	TCP
2024-12-22T09:54:32.844395+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58432	143.119.80.45	37215	TCP
2024-12-22T09:54:32.844500+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46356	157.3.91.94	37215	TCP
2024-12-22T09:54:32.859480+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50730	157.93.80.87	37215	TCP
2024-12-22T09:54:32.859619+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46710	170.117.89.88	37215	TCP
2024-12-22T09:54:32.859774+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45618	197.253.21.39	37215	TCP
2024-12-22T09:54:32.859908+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60840	106.250.214.38	37215	TCP
2024-12-22T09:54:32.860021+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48806	41.202.189.221	37215	TCP
2024-12-22T09:54:32.860070+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43146	197.213.32.2	37215	TCP
2024-12-22T09:54:32.860260+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55828	157.225.103.240	37215	TCP
2024-12-22T09:54:32.860359+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50490	197.116.79.106	37215	TCP
2024-12-22T09:54:32.860423+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41396	197.63.230.149	37215	TCP
2024-12-22T09:54:32.860451+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41690	191.155.104.32	37215	TCP
2024-12-22T09:54:32.860571+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53520	157.107.65.19	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:32.860601+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34560	197.167.68.215	37215	TCP
2024-12-22T09:54:32.860747+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36072	41.145.214.123	37215	TCP
2024-12-22T09:54:32.860777+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54786	190.16.226.175	37215	TCP
2024-12-22T09:54:32.860800+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36590	41.101.2.255	37215	TCP
2024-12-22T09:54:32.860899+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48230	41.193.245.135	37215	TCP
2024-12-22T09:54:32.860971+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48210	83.183.25.243	37215	TCP
2024-12-22T09:54:32.874960+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48408	157.88.5.62	37215	TCP
2024-12-22T09:54:32.875164+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38932	197.66.58.69	37215	TCP
2024-12-22T09:54:32.875170+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41704	41.51.160.41	37215	TCP
2024-12-22T09:54:32.875396+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51620	45.43.197.24	37215	TCP
2024-12-22T09:54:32.875547+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41832	112.55.197.163	37215	TCP
2024-12-22T09:54:32.875616+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34720	197.217.156.54	37215	TCP
2024-12-22T09:54:32.875684+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33414	157.109.168.173	37215	TCP
2024-12-22T09:54:32.875884+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37114	197.176.211.202	37215	TCP
2024-12-22T09:54:32.875972+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48166	155.245.5.80	37215	TCP
2024-12-22T09:54:32.876250+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46826	197.95.102.234	37215	TCP
2024-12-22T09:54:32.876312+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55928	57.120.164.60	37215	TCP
2024-12-22T09:54:32.876431+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41866	41.92.103.130	37215	TCP
2024-12-22T09:54:32.876489+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58048	41.126.50.239	37215	TCP
2024-12-22T09:54:32.876585+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42378	197.121.204.226	37215	TCP
2024-12-22T09:54:32.876866+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43684	41.6.113.145	37215	TCP
2024-12-22T09:54:32.890670+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56794	71.2.188.186	37215	TCP
2024-12-22T09:54:32.890835+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55332	41.82.231.215	37215	TCP
2024-12-22T09:54:32.890857+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54034	41.11.153.105	37215	TCP
2024-12-22T09:54:32.891103+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45006	41.84.131.80	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:32.891131+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36278	197.105.81.129	37215	TCP
2024-12-22T09:54:32.891258+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43190	157.251.189.201	37215	TCP
2024-12-22T09:54:32.891410+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41894	157.149.116.62	37215	TCP
2024-12-22T09:54:32.891437+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49926	188.206.56.235	37215	TCP
2024-12-22T09:54:32.891545+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32868	20.195.212.83	37215	TCP
2024-12-22T09:54:32.891691+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41234	157.178.37.222	37215	TCP
2024-12-22T09:54:32.891795+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46184	150.175.198.56	37215	TCP
2024-12-22T09:54:32.891833+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58888	38.156.221.8	37215	TCP
2024-12-22T09:54:32.938229+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60832	157.141.198.60	37215	TCP
2024-12-22T09:54:32.953310+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58606	197.160.57.98	37215	TCP
2024-12-22T09:54:32.953389+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55084	157.63.107.13	37215	TCP
2024-12-22T09:54:32.954294+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57402	220.230.234.118	37215	TCP
2024-12-22T09:54:32.954493+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47176	41.157.65.27	37215	TCP
2024-12-22T09:54:32.968624+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55934	197.194.90.129	37215	TCP
2024-12-22T09:54:32.968739+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54362	197.167.129.134	37215	TCP
2024-12-22T09:54:32.968804+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47328	125.253.30.17	37215	TCP
2024-12-22T09:54:32.968931+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49418	41.152.28.21	37215	TCP
2024-12-22T09:54:32.968977+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51462	155.217.169.105	37215	TCP
2024-12-22T09:54:32.969129+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42098	223.83.135.244	37215	TCP
2024-12-22T09:54:32.969259+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60706	157.166.215.229	37215	TCP
2024-12-22T09:54:32.969358+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55768	157.209.140.43	37215	TCP
2024-12-22T09:54:32.969580+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48272	37.208.8.186	37215	TCP
2024-12-22T09:54:32.969709+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53078	9.228.193.2	37215	TCP
2024-12-22T09:54:32.969774+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41936	41.65.120.27	37215	TCP
2024-12-22T09:54:32.969871+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53060	157.20.66.146	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:32.970004+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57708	54.168.88.251	37215	TCP
2024-12-22T09:54:32.970308+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53236	197.91.182.226	37215	TCP
2024-12-22T09:54:32.970575+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49552	184.237.113.21	37215	TCP
2024-12-22T09:54:32.984427+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55250	41.10.130.191	37215	TCP
2024-12-22T09:54:32.984659+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38168	197.45.224.37	37215	TCP
2024-12-22T09:54:33.078336+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37172	157.216.217.226	37215	TCP
2024-12-22T09:54:33.078364+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41832	197.115.42.51	37215	TCP
2024-12-22T09:54:33.093956+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32870	197.125.168.173	37215	TCP
2024-12-22T09:54:33.094170+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33600	200.66.53.98	37215	TCP
2024-12-22T09:54:33.094228+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36718	41.66.225.84	37215	TCP
2024-12-22T09:54:33.094230+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34114	197.241.94.41	37215	TCP
2024-12-22T09:54:33.187441+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44512	157.116.180.215	37215	TCP
2024-12-22T09:54:33.203127+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53390	41.139.174.37	37215	TCP
2024-12-22T09:54:33.203280+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46020	157.70.68.103	37215	TCP
2024-12-22T09:54:33.203405+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56278	109.29.181.227	37215	TCP
2024-12-22T09:54:33.203518+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42624	197.21.60.249	37215	TCP
2024-12-22T09:54:33.218701+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35974	158.214.140.26	37215	TCP
2024-12-22T09:54:33.219040+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53498	197.166.76.145	37215	TCP
2024-12-22T09:54:33.219040+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52848	197.19.131.195	37215	TCP
2024-12-22T09:54:33.219064+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39866	157.96.78.80	37215	TCP
2024-12-22T09:54:33.219155+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52814	134.190.208.237	37215	TCP
2024-12-22T09:54:33.219244+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40376	197.136.111.231	37215	TCP
2024-12-22T09:54:33.219424+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35594	197.117.121.5	37215	TCP
2024-12-22T09:54:33.219461+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60434	157.150.148.102	37215	TCP
2024-12-22T09:54:33.219598+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36000	41.131.206.191	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:33.855356+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36138	41.71.163.235	37215	TCP
2024-12-22T09:54:34.096792+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54774	154.114.19.92	37215	TCP
2024-12-22T09:54:34.187779+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57900	41.45.230.95	37215	TCP
2024-12-22T09:54:34.203112+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50960	157.228.237.76	37215	TCP
2024-12-22T09:54:34.203197+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51444	90.42.183.197	37215	TCP
2024-12-22T09:54:34.203204+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52186	41.130.91.234	37215	TCP
2024-12-22T09:54:34.218775+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38266	197.176.208.92	37215	TCP
2024-12-22T09:54:35.015586+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43786	197.137.182.27	37215	TCP
2024-12-22T09:54:35.015730+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59722	73.194.247.19	37215	TCP
2024-12-22T09:54:35.015964+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55320	41.12.222.242	37215	TCP
2024-12-22T09:54:35.016142+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49178	157.184.72.196	37215	TCP
2024-12-22T09:54:35.016287+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54802	23.133.172.170	37215	TCP
2024-12-22T09:54:35.016474+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44552	157.198.235.115	37215	TCP
2024-12-22T09:54:35.016645+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55510	197.143.141.156	37215	TCP
2024-12-22T09:54:35.016912+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57136	157.116.237.232	37215	TCP
2024-12-22T09:54:35.017046+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54298	197.209.12.236	37215	TCP
2024-12-22T09:54:35.017178+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59456	41.77.5.100	37215	TCP
2024-12-22T09:54:35.017295+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41812	96.41.99.37	37215	TCP
2024-12-22T09:54:35.017443+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43884	157.78.16.247	37215	TCP
2024-12-22T09:54:35.017556+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60412	197.126.8.237	37215	TCP
2024-12-22T09:54:35.017597+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42400	197.196.204.10	37215	TCP
2024-12-22T09:54:35.017640+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38806	41.223.59.176	37215	TCP
2024-12-22T09:54:35.017801+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37090	157.229.225.51	37215	TCP
2024-12-22T09:54:35.017927+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55070	41.19.239.36	37215	TCP
2024-12-22T09:54:35.018066+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59812	66.27.238.142	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:35.018184+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57164	157.119.229.47	37215	TCP
2024-12-22T09:54:35.018300+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37172	157.105.228.121	37215	TCP
2024-12-22T09:54:35.018381+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36022	41.55.243.171	37215	TCP
2024-12-22T09:54:35.018559+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48992	157.219.217.229	37215	TCP
2024-12-22T09:54:35.018664+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43212	157.217.70.147	37215	TCP
2024-12-22T09:54:35.018836+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51116	157.231.177.245	37215	TCP
2024-12-22T09:54:35.018891+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46944	157.254.42.112	37215	TCP
2024-12-22T09:54:35.031246+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38300	157.19.62.171	37215	TCP
2024-12-22T09:54:35.031323+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47582	140.185.220.66	37215	TCP
2024-12-22T09:54:35.031425+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49466	197.149.147.88	37215	TCP
2024-12-22T09:54:35.031610+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45672	41.76.99.195	37215	TCP
2024-12-22T09:54:35.031739+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48098	199.236.111.157	37215	TCP
2024-12-22T09:54:35.062453+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60920	157.49.241.166	37215	TCP
2024-12-22T09:54:35.062579+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35224	157.92.30.133	37215	TCP
2024-12-22T09:54:35.062710+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32856	197.120.129.255	37215	TCP
2024-12-22T09:54:35.062800+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37374	41.172.79.137	37215	TCP
2024-12-22T09:54:35.062825+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51306	157.13.225.74	37215	TCP
2024-12-22T09:54:35.062959+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43046	157.102.98.62	37215	TCP
2024-12-22T09:54:35.063089+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58038	197.128.198.210	37215	TCP
2024-12-22T09:54:35.063254+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41724	41.133.133.181	37215	TCP
2024-12-22T09:54:35.063390+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53058	41.48.174.32	37215	TCP
2024-12-22T09:54:35.063485+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57492	223.18.187.215	37215	TCP
2024-12-22T09:54:35.063646+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34370	157.210.177.65	37215	TCP
2024-12-22T09:54:35.063727+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33028	197.142.151.217	37215	TCP
2024-12-22T09:54:35.063890+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38872	197.207.124.159	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:35.063998+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51876	41.26.61.237	37215	TCP
2024-12-22T09:54:35.064095+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58486	138.226.78.54	37215	TCP
2024-12-22T09:54:35.064171+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44510	41.76.76.62	37215	TCP
2024-12-22T09:54:35.064298+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40212	41.241.124.45	37215	TCP
2024-12-22T09:54:35.064515+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37240	157.12.60.128	37215	TCP
2024-12-22T09:54:35.064636+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38952	123.109.145.174	37215	TCP
2024-12-22T09:54:35.064699+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53140	206.133.93.70	37215	TCP
2024-12-22T09:54:35.064924+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60042	157.181.139.67	37215	TCP
2024-12-22T09:54:35.065019+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41618	197.211.166.214	37215	TCP
2024-12-22T09:54:35.065132+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40336	43.19.29.173	37215	TCP
2024-12-22T09:54:35.065224+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32922	197.61.225.161	37215	TCP
2024-12-22T09:54:35.065275+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60282	197.236.125.148	37215	TCP
2024-12-22T09:54:35.065341+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47882	157.146.13.88	37215	TCP
2024-12-22T09:54:35.065490+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38366	74.210.170.36	37215	TCP
2024-12-22T09:54:35.065631+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49784	157.159.28.214	37215	TCP
2024-12-22T09:54:35.065673+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33332	25.39.229.133	37215	TCP
2024-12-22T09:54:35.065743+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58808	190.186.151.60	37215	TCP
2024-12-22T09:54:35.065846+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53186	157.165.13.125	37215	TCP
2024-12-22T09:54:35.065940+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43734	157.77.6.112	37215	TCP
2024-12-22T09:54:35.066019+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55906	197.58.253.179	37215	TCP
2024-12-22T09:54:35.066128+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58914	197.123.83.143	37215	TCP
2024-12-22T09:54:35.066161+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42826	41.46.120.193	37215	TCP
2024-12-22T09:54:35.066263+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43170	217.175.106.75	37215	TCP
2024-12-22T09:54:35.066306+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44410	188.133.186.239	37215	TCP
2024-12-22T09:54:35.068028+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45784	197.131.153.162	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:35.156005+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60208	141.162.146.172	37215	TCP
2024-12-22T09:54:35.156122+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57812	157.93.235.58	37215	TCP
2024-12-22T09:54:35.156237+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52840	216.211.132.202	37215	TCP
2024-12-22T09:54:35.187462+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59038	93.171.13.0	37215	TCP
2024-12-22T09:54:35.187605+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50006	152.15.160.101	37215	TCP
2024-12-22T09:54:35.187728+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59948	174.56.71.142	37215	TCP
2024-12-22T09:54:35.265694+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36636	197.123.110.112	37215	TCP
2024-12-22T09:54:35.265840+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56106	197.70.237.1	37215	TCP
2024-12-22T09:54:35.281200+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37088	197.210.136.112	37215	TCP
2024-12-22T09:54:35.281291+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39872	157.248.254.241	37215	TCP
2024-12-22T09:54:35.281447+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51520	157.207.218.36	37215	TCP
2024-12-22T09:54:35.296777+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35244	41.168.233.196	37215	TCP
2024-12-22T09:54:36.156510+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36214	84.172.12.182	37215	TCP
2024-12-22T09:54:36.156588+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49024	197.5.193.200	37215	TCP
2024-12-22T09:54:36.156598+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41388	113.244.68.174	37215	TCP
2024-12-22T09:54:36.156609+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43710	41.57.139.31	37215	TCP
2024-12-22T09:54:36.156696+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51100	157.180.238.38	37215	TCP
2024-12-22T09:54:36.156790+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32938	41.129.63.233	37215	TCP
2024-12-22T09:54:36.156910+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57892	157.225.139.208	37215	TCP
2024-12-22T09:54:36.157136+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60154	157.140.131.136	37215	TCP
2024-12-22T09:54:36.157280+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49096	157.46.7.49	37215	TCP
2024-12-22T09:54:36.171799+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41052	157.216.75.179	37215	TCP
2024-12-22T09:54:36.171999+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50546	197.79.17.131	37215	TCP
2024-12-22T09:54:36.172022+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43388	20.230.182.145	37215	TCP
2024-12-22T09:54:36.172110+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49258	41.202.129.65	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:36.172290+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49382	197.199.243.49	37215	TCP
2024-12-22T09:54:36.172457+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48706	220.54.189.215	37215	TCP
2024-12-22T09:54:36.172540+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41986	74.211.127.9	37215	TCP
2024-12-22T09:54:36.172643+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51224	197.19.114.32	37215	TCP
2024-12-22T09:54:36.172727+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56368	41.144.99.10	37215	TCP
2024-12-22T09:54:36.172822+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43682	41.143.239.184	37215	TCP
2024-12-22T09:54:36.172983+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47290	197.103.143.48	37215	TCP
2024-12-22T09:54:36.173108+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47150	197.129.74.251	37215	TCP
2024-12-22T09:54:36.173317+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55010	197.115.106.116	37215	TCP
2024-12-22T09:54:36.173443+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58072	157.31.163.165	37215	TCP
2024-12-22T09:54:36.173554+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43322	41.206.177.175	37215	TCP
2024-12-22T09:54:36.173675+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45814	213.133.46.194	37215	TCP
2024-12-22T09:54:36.173776+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33538	157.149.125.151	37215	TCP
2024-12-22T09:54:36.173850+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54306	123.74.154.250	37215	TCP
2024-12-22T09:54:36.173934+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58932	197.88.247.123	37215	TCP
2024-12-22T09:54:36.174006+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53750	197.95.53.45	37215	TCP
2024-12-22T09:54:36.174096+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33504	41.42.42.128	37215	TCP
2024-12-22T09:54:36.174193+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59326	157.66.120.23	37215	TCP
2024-12-22T09:54:36.174285+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57692	150.23.156.8	37215	TCP
2024-12-22T09:54:36.174395+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55000	197.181.46.251	37215	TCP
2024-12-22T09:54:36.174515+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40602	89.143.85.248	37215	TCP
2024-12-22T09:54:36.174628+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43628	157.226.248.132	37215	TCP
2024-12-22T09:54:36.174707+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38710	157.52.98.77	37215	TCP
2024-12-22T09:54:36.174783+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54394	41.130.109.164	37215	TCP
2024-12-22T09:54:36.174874+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58316	157.33.176.94	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:36.174956+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59478	157.146.236.76	37215	TCP
2024-12-22T09:54:36.175050+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55054	80.128.9.77	37215	TCP
2024-12-22T09:54:36.175463+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46392	157.30.251.95	37215	TCP
2024-12-22T09:54:36.175554+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44140	157.99.47.57	37215	TCP
2024-12-22T09:54:36.175587+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49564	197.56.223.242	37215	TCP
2024-12-22T09:54:36.175717+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58066	41.104.94.89	37215	TCP
2024-12-22T09:54:36.187303+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57112	41.121.204.244	37215	TCP
2024-12-22T09:54:36.187412+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49216	197.187.64.94	37215	TCP
2024-12-22T09:54:36.187558+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54736	157.113.254.70	37215	TCP
2024-12-22T09:54:36.187670+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48778	157.39.63.65	37215	TCP
2024-12-22T09:54:36.187791+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42164	207.42.247.33	37215	TCP
2024-12-22T09:54:36.187931+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47330	41.69.134.82	37215	TCP
2024-12-22T09:54:36.187976+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45224	197.3.134.64	37215	TCP
2024-12-22T09:54:36.202948+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56592	157.148.151.222	37215	TCP
2024-12-22T09:54:36.203144+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33106	157.50.158.175	37215	TCP
2024-12-22T09:54:36.203160+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37342	197.85.116.249	37215	TCP
2024-12-22T09:54:36.203335+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44408	68.175.86.152	37215	TCP
2024-12-22T09:54:36.203344+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45638	157.156.242.16	37215	TCP
2024-12-22T09:54:36.203460+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58870	197.241.145.155	37215	TCP
2024-12-22T09:54:36.203534+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46448	146.198.245.6	37215	TCP
2024-12-22T09:54:36.203615+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51296	197.52.110.114	37215	TCP
2024-12-22T09:54:36.203707+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53462	45.126.101.33	37215	TCP
2024-12-22T09:54:36.203993+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42106	157.11.3.59	37215	TCP
2024-12-22T09:54:36.204122+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35778	41.126.91.241	37215	TCP
2024-12-22T09:54:36.204151+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50852	197.201.157.89	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:36.204225+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51098	197.141.192.167	37215	TCP
2024-12-22T09:54:36.218700+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53992	157.85.207.129	37215	TCP
2024-12-22T09:54:36.218947+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48232	41.58.181.104	37215	TCP
2024-12-22T09:54:36.218956+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54074	43.107.99.245	37215	TCP
2024-12-22T09:54:36.219043+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38812	197.0.111.119	37215	TCP
2024-12-22T09:54:36.219138+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45988	197.55.134.216	37215	TCP
2024-12-22T09:54:36.219298+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40062	96.92.59.70	37215	TCP
2024-12-22T09:54:36.219353+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35640	197.158.250.182	37215	TCP
2024-12-22T09:54:36.219456+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41324	157.215.27.64	37215	TCP
2024-12-22T09:54:36.219556+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48732	85.53.135.10	37215	TCP
2024-12-22T09:54:36.219658+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52920	41.138.111.184	37215	TCP
2024-12-22T09:54:36.219759+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44534	157.28.54.168	37215	TCP
2024-12-22T09:54:36.220098+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37598	157.237.6.220	37215	TCP
2024-12-22T09:54:36.220270+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33984	41.144.133.216	37215	TCP
2024-12-22T09:54:36.220298+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59166	137.105.247.184	37215	TCP
2024-12-22T09:54:36.220399+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54760	157.154.79.80	37215	TCP
2024-12-22T09:54:36.220528+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53696	157.98.253.164	37215	TCP
2024-12-22T09:54:36.220631+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41120	193.85.48.73	37215	TCP
2024-12-22T09:54:36.220732+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37602	157.141.157.83	37215	TCP
2024-12-22T09:54:36.220842+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59800	41.23.147.191	37215	TCP
2024-12-22T09:54:36.220933+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33532	93.177.177.212	37215	TCP
2024-12-22T09:54:36.221031+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37348	157.156.45.70	37215	TCP
2024-12-22T09:54:36.221123+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52508	157.244.111.60	37215	TCP
2024-12-22T09:54:36.221232+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49396	41.26.240.145	37215	TCP
2024-12-22T09:54:36.221259+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55602	157.113.226.117	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:36.221408+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38818	197.9.181.58	37215	TCP
2024-12-22T09:54:36.221507+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36956	157.88.169.191	37215	TCP
2024-12-22T09:54:36.234215+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49522	41.160.148.227	37215	TCP
2024-12-22T09:54:36.234337+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54926	157.192.108.52	37215	TCP
2024-12-22T09:54:36.234477+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44946	41.44.4.244	37215	TCP
2024-12-22T09:54:36.234570+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51342	157.128.85.66	37215	TCP
2024-12-22T09:54:36.296856+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45388	41.17.162.79	37215	TCP
2024-12-22T09:54:36.406209+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48336	41.65.254.41	37215	TCP
2024-12-22T09:54:36.406281+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41132	157.119.10.131	37215	TCP
2024-12-22T09:54:36.406413+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32808	126.228.223.35	37215	TCP
2024-12-22T09:54:36.406457+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50430	207.186.61.146	37215	TCP
2024-12-22T09:54:36.437518+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37044	41.183.49.72	37215	TCP
2024-12-22T09:54:36.437657+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35988	205.46.48.39	37215	TCP
2024-12-22T09:54:37.456492+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54630	219.85.237.133	37215	TCP
2024-12-22T09:54:38.187922+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52576	197.10.9.135	37215	TCP
2024-12-22T09:54:38.187922+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40022	157.220.98.251	37215	TCP
2024-12-22T09:54:38.203238+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46546	157.217.224.59	37215	TCP
2024-12-22T09:54:38.203413+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45006	197.29.215.218	37215	TCP
2024-12-22T09:54:38.218818+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48668	157.174.103.141	37215	TCP
2024-12-22T09:54:38.218818+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39128	196.34.166.220	37215	TCP
2024-12-22T09:54:38.328193+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37516	211.252.175.92	37215	TCP
2024-12-22T09:54:38.343986+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34272	197.222.205.230	37215	TCP
2024-12-22T09:54:38.343990+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43668	197.43.103.180	37215	TCP
2024-12-22T09:54:38.343996+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41732	197.104.116.144	37215	TCP
2024-12-22T09:54:38.344102+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56522	197.162.42.120	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.344255+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38344	172.245.106.1	37215	TCP
2024-12-22T09:54:38.344382+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56352	41.172.13.39	37215	TCP
2024-12-22T09:54:38.344509+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37956	197.60.60.16	37215	TCP
2024-12-22T09:54:38.344691+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48682	157.37.50.166	37215	TCP
2024-12-22T09:54:38.344972+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47942	41.43.13.26	37215	TCP
2024-12-22T09:54:38.345096+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34058	157.94.171.73	37215	TCP
2024-12-22T09:54:38.345164+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48076	119.106.145.205	37215	TCP
2024-12-22T09:54:38.345344+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44658	41.82.149.155	37215	TCP
2024-12-22T09:54:38.356089+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50986	197.238.212.204	37215	TCP
2024-12-22T09:54:38.356151+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37376	197.38.185.22	37215	TCP
2024-12-22T09:54:38.356202+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36858	41.50.67.148	37215	TCP
2024-12-22T09:54:38.356341+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37230	64.47.250.112	37215	TCP
2024-12-22T09:54:38.359191+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40634	41.231.51.216	37215	TCP
2024-12-22T09:54:38.359357+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52076	157.170.143.128	37215	TCP
2024-12-22T09:54:38.359471+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41150	197.7.18.61	37215	TCP
2024-12-22T09:54:38.359588+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38800	41.188.73.193	37215	TCP
2024-12-22T09:54:38.359709+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51928	41.214.193.173	37215	TCP
2024-12-22T09:54:38.359872+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46412	137.44.18.179	37215	TCP
2024-12-22T09:54:38.359956+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36760	83.41.195.201	37215	TCP
2024-12-22T09:54:38.360106+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55416	197.40.207.53	37215	TCP
2024-12-22T09:54:38.360273+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35638	197.241.179.130	37215	TCP
2024-12-22T09:54:38.360584+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53736	41.217.103.0	37215	TCP
2024-12-22T09:54:38.360742+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55954	157.190.234.237	37215	TCP
2024-12-22T09:54:38.360877+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36814	197.8.58.127	37215	TCP
2024-12-22T09:54:38.361026+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54190	40.120.46.26	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.361147+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58608	157.89.191.234	37215	TCP
2024-12-22T09:54:38.361182+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42218	175.183.217.123	37215	TCP
2024-12-22T09:54:38.361303+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47478	86.219.171.106	37215	TCP
2024-12-22T09:54:38.361395+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57998	204.18.4.163	37215	TCP
2024-12-22T09:54:38.361588+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43748	197.239.208.39	37215	TCP
2024-12-22T09:54:38.361734+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40698	197.230.213.167	37215	TCP
2024-12-22T09:54:38.361865+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32814	46.99.172.115	37215	TCP
2024-12-22T09:54:38.361925+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38974	41.32.177.151	37215	TCP
2024-12-22T09:54:38.362084+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34670	157.182.252.124	37215	TCP
2024-12-22T09:54:38.362188+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44092	122.91.199.102	37215	TCP
2024-12-22T09:54:38.362358+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41566	40.46.160.129	37215	TCP
2024-12-22T09:54:38.362411+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51520	167.228.57.6	37215	TCP
2024-12-22T09:54:38.362501+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52202	41.54.171.10	37215	TCP
2024-12-22T09:54:38.362563+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57418	148.189.102.87	37215	TCP
2024-12-22T09:54:38.362671+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60630	157.82.149.3	37215	TCP
2024-12-22T09:54:38.362926+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50850	197.87.191.59	37215	TCP
2024-12-22T09:54:38.363093+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47032	58.45.181.81	37215	TCP
2024-12-22T09:54:38.363145+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46110	41.188.16.55	37215	TCP
2024-12-22T09:54:38.363250+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39302	157.102.9.38	37215	TCP
2024-12-22T09:54:38.390554+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50206	206.72.181.115	37215	TCP
2024-12-22T09:54:38.429019+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38054	41.9.137.61	37215	TCP
2024-12-22T09:54:38.429056+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56418	41.37.164.157	37215	TCP
2024-12-22T09:54:38.429086+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38128	205.171.75.214	37215	TCP
2024-12-22T09:54:38.437320+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47382	41.139.112.115	37215	TCP
2024-12-22T09:54:38.437425+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42898	157.119.150.238	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.437595+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33174	46.103.23.179	37215	TCP
2024-12-22T09:54:38.437668+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53776	41.203.206.27	37215	TCP
2024-12-22T09:54:38.437911+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36566	197.86.86.40	37215	TCP
2024-12-22T09:54:38.438150+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58878	192.12.52.5	37215	TCP
2024-12-22T09:54:38.438267+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35468	41.161.30.26	37215	TCP
2024-12-22T09:54:38.438299+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51360	1.69.55.80	37215	TCP
2024-12-22T09:54:38.438454+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50712	197.107.36.10	37215	TCP
2024-12-22T09:54:38.438583+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42370	41.72.129.236	37215	TCP
2024-12-22T09:54:38.438708+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37964	41.31.143.8	37215	TCP
2024-12-22T09:54:38.438820+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58442	41.43.110.134	37215	TCP
2024-12-22T09:54:38.438933+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56912	197.88.252.222	37215	TCP
2024-12-22T09:54:38.439013+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49854	197.185.171.75	37215	TCP
2024-12-22T09:54:38.439081+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59214	152.224.192.122	37215	TCP
2024-12-22T09:54:38.439226+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59162	41.185.22.109	37215	TCP
2024-12-22T09:54:38.439366+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33748	197.114.162.167	37215	TCP
2024-12-22T09:54:38.439465+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46360	201.75.163.101	37215	TCP
2024-12-22T09:54:38.439588+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59692	197.145.57.186	37215	TCP
2024-12-22T09:54:38.439605+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56250	134.71.74.92	37215	TCP
2024-12-22T09:54:38.439754+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37418	41.9.170.50	37215	TCP
2024-12-22T09:54:38.439879+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40418	157.100.62.149	37215	TCP
2024-12-22T09:54:38.439959+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48536	157.47.139.221	37215	TCP
2024-12-22T09:54:38.440018+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37880	157.61.121.161	37215	TCP
2024-12-22T09:54:38.440122+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35668	157.202.180.151	37215	TCP
2024-12-22T09:54:38.440406+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45732	157.236.88.63	37215	TCP
2024-12-22T09:54:38.440527+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35824	41.212.130.32	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.440698+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34240	197.214.202.165	37215	TCP
2024-12-22T09:54:38.453535+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51004	120.75.13.116	37215	TCP
2024-12-22T09:54:38.453721+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49668	157.111.225.114	37215	TCP
2024-12-22T09:54:38.453903+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38526	41.164.167.173	37215	TCP
2024-12-22T09:54:38.453958+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42218	197.176.188.167	37215	TCP
2024-12-22T09:54:38.454059+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34212	157.206.216.143	37215	TCP
2024-12-22T09:54:38.454128+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54264	157.85.229.12	37215	TCP
2024-12-22T09:54:38.454241+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49808	197.82.91.205	37215	TCP
2024-12-22T09:54:38.454362+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44526	197.211.40.53	37215	TCP
2024-12-22T09:54:38.468762+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40686	206.212.28.113	37215	TCP
2024-12-22T09:54:38.468995+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55886	41.198.77.226	37215	TCP
2024-12-22T09:54:38.469003+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53742	98.3.110.46	37215	TCP
2024-12-22T09:54:38.469136+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52638	157.143.19.134	37215	TCP
2024-12-22T09:54:38.469233+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41116	157.199.173.146	37215	TCP
2024-12-22T09:54:38.469302+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50728	157.230.219.236	37215	TCP
2024-12-22T09:54:38.469390+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47832	197.244.78.206	37215	TCP
2024-12-22T09:54:38.469508+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44542	157.23.136.155	37215	TCP
2024-12-22T09:54:38.469612+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47896	41.116.123.134	37215	TCP
2024-12-22T09:54:38.469770+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48872	41.126.14.168	37215	TCP
2024-12-22T09:54:38.469840+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38988	197.88.171.122	37215	TCP
2024-12-22T09:54:38.469920+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53636	157.9.52.41	37215	TCP
2024-12-22T09:54:38.470045+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56054	197.33.142.56	37215	TCP
2024-12-22T09:54:38.470138+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45336	197.112.91.61	37215	TCP
2024-12-22T09:54:38.470299+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46262	65.206.81.30	37215	TCP
2024-12-22T09:54:38.470403+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48860	41.83.51.17	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.470431+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39802	9.3.82.165	37215	TCP
2024-12-22T09:54:38.470530+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33276	41.105.147.157	37215	TCP
2024-12-22T09:54:38.470632+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50138	157.41.197.149	37215	TCP
2024-12-22T09:54:38.484396+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48950	157.178.87.150	37215	TCP
2024-12-22T09:54:38.484518+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43568	41.6.225.193	37215	TCP
2024-12-22T09:54:38.484642+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39782	197.213.36.103	37215	TCP
2024-12-22T09:54:38.484759+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35618	157.221.20.255	37215	TCP
2024-12-22T09:54:38.484854+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54922	41.135.226.124	37215	TCP
2024-12-22T09:54:38.484952+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36756	157.119.24.24	37215	TCP
2024-12-22T09:54:38.485081+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59386	41.176.205.103	37215	TCP
2024-12-22T09:54:38.485323+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40930	197.123.199.156	37215	TCP
2024-12-22T09:54:38.485437+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47040	41.1.23.104	37215	TCP
2024-12-22T09:54:38.485551+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39024	62.66.90.167	37215	TCP
2024-12-22T09:54:38.485674+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39680	41.58.157.153	37215	TCP
2024-12-22T09:54:38.485792+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44958	197.88.108.124	37215	TCP
2024-12-22T09:54:38.485978+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58512	197.209.137.164	37215	TCP
2024-12-22T09:54:38.486095+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42062	157.89.253.41	37215	TCP
2024-12-22T09:54:38.486218+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41806	202.154.54.63	37215	TCP
2024-12-22T09:54:38.486334+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36532	157.35.124.193	37215	TCP
2024-12-22T09:54:38.486462+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40484	197.60.151.237	37215	TCP
2024-12-22T09:54:38.486577+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38496	147.130.1.100	37215	TCP
2024-12-22T09:54:38.486623+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33882	197.15.81.135	37215	TCP
2024-12-22T09:54:38.486721+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41916	157.252.209.81	37215	TCP
2024-12-22T09:54:38.486822+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40752	2.107.168.123	37215	TCP
2024-12-22T09:54:38.486949+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37964	197.192.126.208	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.487042+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37362	166.208.171.185	37215	TCP
2024-12-22T09:54:38.487123+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58122	101.53.29.54	37215	TCP
2024-12-22T09:54:38.487273+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45678	41.195.133.181	37215	TCP
2024-12-22T09:54:38.487520+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58470	72.77.130.129	37215	TCP
2024-12-22T09:54:38.487622+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39124	41.28.1.80	37215	TCP
2024-12-22T09:54:38.487731+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46102	223.60.55.208	37215	TCP
2024-12-22T09:54:38.487888+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55380	197.155.18.234	37215	TCP
2024-12-22T09:54:38.487978+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50520	41.82.37.74	37215	TCP
2024-12-22T09:54:38.488079+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56632	185.190.246.117	37215	TCP
2024-12-22T09:54:38.488213+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55510	65.29.142.24	37215	TCP
2024-12-22T09:54:38.488333+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59662	41.96.144.190	37215	TCP
2024-12-22T09:54:38.488425+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36102	197.28.112.45	37215	TCP
2024-12-22T09:54:38.488522+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54712	41.80.63.229	37215	TCP
2024-12-22T09:54:38.488615+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43050	157.113.86.82	37215	TCP
2024-12-22T09:54:38.488682+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34920	157.117.2.25	37215	TCP
2024-12-22T09:54:38.488801+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57094	157.96.66.232	37215	TCP
2024-12-22T09:54:38.488916+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57754	157.148.174.120	37215	TCP
2024-12-22T09:54:38.488979+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42834	197.10.229.114	37215	TCP
2024-12-22T09:54:38.489085+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52612	157.72.118.234	37215	TCP
2024-12-22T09:54:38.489208+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35226	197.233.125.34	37215	TCP
2024-12-22T09:54:38.489275+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43832	41.153.102.92	37215	TCP
2024-12-22T09:54:38.489503+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45544	157.91.8.252	37215	TCP
2024-12-22T09:54:38.489541+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41764	41.14.84.14	37215	TCP
2024-12-22T09:54:38.489633+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51958	41.167.189.101	37215	TCP
2024-12-22T09:54:38.489744+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58380	13.90.196.182	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.489872+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60500	157.112.136.25	37215	TCP
2024-12-22T09:54:38.489954+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35046	197.181.68.93	37215	TCP
2024-12-22T09:54:38.490028+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55922	93.134.187.80	37215	TCP
2024-12-22T09:54:38.490116+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54288	197.246.129.216	37215	TCP
2024-12-22T09:54:38.490230+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54276	197.48.55.68	37215	TCP
2024-12-22T09:54:38.490259+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40286	157.175.245.169	37215	TCP
2024-12-22T09:54:38.490463+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48182	197.12.78.27	37215	TCP
2024-12-22T09:54:38.490574+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58876	197.244.248.146	37215	TCP
2024-12-22T09:54:38.490631+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60800	27.123.199.8	37215	TCP
2024-12-22T09:54:38.490693+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44004	192.162.61.139	37215	TCP
2024-12-22T09:54:38.490787+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55206	177.154.80.115	37215	TCP
2024-12-22T09:54:38.490893+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36358	197.170.64.62	37215	TCP
2024-12-22T09:54:38.490925+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34886	157.242.210.47	37215	TCP
2024-12-22T09:54:38.491018+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59862	197.201.55.176	37215	TCP
2024-12-22T09:54:38.491126+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37832	61.32.33.34	37215	TCP
2024-12-22T09:54:38.491237+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55272	197.243.158.108	37215	TCP
2024-12-22T09:54:38.491348+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36004	197.149.2.90	37215	TCP
2024-12-22T09:54:38.491410+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54562	41.213.61.71	37215	TCP
2024-12-22T09:54:38.491531+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47926	216.62.186.126	37215	TCP
2024-12-22T09:54:38.491649+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33712	41.170.6.36	37215	TCP
2024-12-22T09:54:38.491721+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45092	157.2.90.13	37215	TCP
2024-12-22T09:54:38.491842+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34662	41.88.74.242	37215	TCP
2024-12-22T09:54:38.492015+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38300	41.4.80.228	37215	TCP
2024-12-22T09:54:38.492141+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54664	41.46.35.48	37215	TCP
2024-12-22T09:54:38.492277+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56548	197.40.17.236	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.492381+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48452	157.190.146.59	37215	TCP
2024-12-22T09:54:38.492463+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42300	197.26.228.143	37215	TCP
2024-12-22T09:54:38.492506+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49442	41.231.143.124	37215	TCP
2024-12-22T09:54:38.492605+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41692	41.129.79.156	37215	TCP
2024-12-22T09:54:38.492697+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51752	157.76.202.27	37215	TCP
2024-12-22T09:54:38.492793+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41094	157.243.142.130	37215	TCP
2024-12-22T09:54:38.492895+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41712	1.99.134.121	37215	TCP
2024-12-22T09:54:38.493073+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39838	41.144.213.56	37215	TCP
2024-12-22T09:54:38.493190+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51692	197.221.43.146	37215	TCP
2024-12-22T09:54:38.493224+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54296	41.35.55.253	37215	TCP
2024-12-22T09:54:38.493290+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60062	197.31.74.2	37215	TCP
2024-12-22T09:54:38.493376+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59262	157.140.99.31	37215	TCP
2024-12-22T09:54:38.493606+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57564	157.243.3.139	37215	TCP
2024-12-22T09:54:38.493699+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44964	197.146.185.193	37215	TCP
2024-12-22T09:54:38.493781+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41146	41.14.115.66	37215	TCP
2024-12-22T09:54:38.493888+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52038	41.71.41.176	37215	TCP
2024-12-22T09:54:38.493998+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34270	102.93.162.142	37215	TCP
2024-12-22T09:54:38.494069+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55844	41.207.190.237	37215	TCP
2024-12-22T09:54:38.494146+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54770	157.209.99.126	37215	TCP
2024-12-22T09:54:38.494251+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36960	197.245.24.42	37215	TCP
2024-12-22T09:54:38.494421+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55092	157.219.220.114	37215	TCP
2024-12-22T09:54:38.494545+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37358	213.25.62.71	37215	TCP
2024-12-22T09:54:38.494576+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33120	197.105.75.172	37215	TCP
2024-12-22T09:54:38.494669+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56986	197.52.126.211	37215	TCP
2024-12-22T09:54:38.495104+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43364	41.9.105.19	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.495249+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54992	41.10.198.166	37215	TCP
2024-12-22T09:54:38.495379+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46252	157.3.99.90	37215	TCP
2024-12-22T09:54:38.495411+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39340	41.107.251.32	37215	TCP
2024-12-22T09:54:38.495497+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33988	218.131.124.172	37215	TCP
2024-12-22T09:54:38.495630+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46728	96.225.10.71	37215	TCP
2024-12-22T09:54:38.495741+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58840	41.237.39.152	37215	TCP
2024-12-22T09:54:38.495900+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34540	89.107.191.235	37215	TCP
2024-12-22T09:54:38.495986+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42430	73.236.146.240	37215	TCP
2024-12-22T09:54:38.496081+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60908	157.71.90.84	37215	TCP
2024-12-22T09:54:38.496137+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42170	157.78.27.118	37215	TCP
2024-12-22T09:54:38.496227+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52476	41.74.127.201	37215	TCP
2024-12-22T09:54:38.496319+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59638	168.9.251.160	37215	TCP
2024-12-22T09:54:38.496427+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39538	197.204.142.41	37215	TCP
2024-12-22T09:54:38.496495+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38768	157.246.222.210	37215	TCP
2024-12-22T09:54:38.496588+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58432	197.49.210.133	37215	TCP
2024-12-22T09:54:38.496748+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56604	157.99.0.5	37215	TCP
2024-12-22T09:54:38.496850+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34850	157.114.239.129	37215	TCP
2024-12-22T09:54:38.496879+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48056	41.252.95.64	37215	TCP
2024-12-22T09:54:38.496919+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34202	197.143.191.215	37215	TCP
2024-12-22T09:54:38.496979+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50740	197.53.200.178	37215	TCP
2024-12-22T09:54:38.497075+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54776	41.4.212.117	37215	TCP
2024-12-22T09:54:38.497171+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56550	204.60.41.96	37215	TCP
2024-12-22T09:54:38.497332+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44100	44.195.26.98	37215	TCP
2024-12-22T09:54:38.497502+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37608	200.144.159.121	37215	TCP
2024-12-22T09:54:38.497526+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55670	41.13.211.217	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:38.515625+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37368	59.150.13.216	37215	TCP
2024-12-22T09:54:38.515968+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37132	41.38.58.97	37215	TCP
2024-12-22T09:54:38.515988+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47290	169.214.116.84	37215	TCP
2024-12-22T09:54:38.516022+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34306	41.253.208.36	37215	TCP
2024-12-22T09:54:38.516428+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58068	125.116.98.8	37215	TCP
2024-12-22T09:54:38.516537+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42002	72.242.27.0	37215	TCP
2024-12-22T09:54:38.516688+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52388	41.81.204.117	37215	TCP
2024-12-22T09:54:38.516848+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32886	157.140.54.232	37215	TCP
2024-12-22T09:54:38.517111+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50986	145.231.85.209	37215	TCP
2024-12-22T09:54:38.517257+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35894	149.150.35.157	37215	TCP
2024-12-22T09:54:38.517373+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48102	157.218.145.184	37215	TCP
2024-12-22T09:54:38.517468+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41426	166.22.215.243	37215	TCP
2024-12-22T09:54:38.517619+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58076	197.142.192.249	37215	TCP
2024-12-22T09:54:38.517824+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47098	41.55.41.127	37215	TCP
2024-12-22T09:54:38.518010+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38174	157.112.144.13	37215	TCP
2024-12-22T09:54:38.518255+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50126	118.74.60.100	37215	TCP
2024-12-22T09:54:38.518362+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51462	157.16.108.38	37215	TCP
2024-12-22T09:54:38.518655+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49354	157.100.25.0	37215	TCP
2024-12-22T09:54:38.518855+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36596	41.217.226.146	37215	TCP
2024-12-22T09:54:38.518996+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44932	41.135.6.82	37215	TCP
2024-12-22T09:54:38.546751+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42244	41.25.226.250	37215	TCP
2024-12-22T09:54:38.869555+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40528	41.190.102.15	37215	TCP
2024-12-22T09:54:40.607511+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59610	124.56.12.207	37215	TCP
2024-12-22T09:54:40.781468+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41512	182.67.182.239	37215	TCP
2024-12-22T09:54:40.781479+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37352	197.206.178.124	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:40.781548+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35194	197.94.246.245	37215	TCP
2024-12-22T09:54:40.781792+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55514	197.133.226.219	37215	TCP
2024-12-22T09:54:40.781963+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33742	41.38.152.172	37215	TCP
2024-12-22T09:54:40.782200+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57400	197.123.182.53	37215	TCP
2024-12-22T09:54:40.782348+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52822	41.116.195.79	37215	TCP
2024-12-22T09:54:40.782483+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44960	41.88.192.239	37215	TCP
2024-12-22T09:54:40.782611+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58944	197.117.106.197	37215	TCP
2024-12-22T09:54:40.783091+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35398	42.216.162.168	37215	TCP
2024-12-22T09:54:40.783131+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36800	157.46.40.255	37215	TCP
2024-12-22T09:54:40.783260+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53260	157.250.128.244	37215	TCP
2024-12-22T09:54:40.783409+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40598	157.137.156.165	37215	TCP
2024-12-22T09:54:40.783581+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53628	157.61.65.41	37215	TCP
2024-12-22T09:54:40.783662+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57454	197.250.38.147	37215	TCP
2024-12-22T09:54:40.783869+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55486	41.210.110.36	37215	TCP
2024-12-22T09:54:40.783902+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57470	157.238.227.136	37215	TCP
2024-12-22T09:54:40.783949+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44884	77.78.75.11	37215	TCP
2024-12-22T09:54:40.784179+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56400	157.164.243.5	37215	TCP
2024-12-22T09:54:40.784443+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56608	83.251.205.79	37215	TCP
2024-12-22T09:54:40.784607+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45808	157.193.221.66	37215	TCP
2024-12-22T09:54:40.812520+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56542	157.26.190.153	37215	TCP
2024-12-22T09:54:40.812650+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44902	44.217.2.246	37215	TCP
2024-12-22T09:54:40.812738+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60744	46.237.90.246	37215	TCP
2024-12-22T09:54:40.812826+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46716	87.189.117.106	37215	TCP
2024-12-22T09:54:40.812944+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44232	157.184.104.236	37215	TCP
2024-12-22T09:54:40.813048+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60654	41.96.22.70	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:40.813154+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37556	157.24.162.212	37215	TCP
2024-12-22T09:54:40.813313+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57546	41.248.52.181	37215	TCP
2024-12-22T09:54:40.813447+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58998	186.74.79.219	37215	TCP
2024-12-22T09:54:40.813691+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49818	167.206.120.16	37215	TCP
2024-12-22T09:54:40.890916+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34890	157.104.26.138	37215	TCP
2024-12-22T09:54:40.906322+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37134	41.242.37.115	37215	TCP
2024-12-22T09:54:40.906499+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50736	41.24.255.232	37215	TCP
2024-12-22T09:54:40.906650+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48592	41.25.2.169	37215	TCP
2024-12-22T09:54:40.906850+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38296	79.173.82.161	37215	TCP
2024-12-22T09:54:40.906866+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57404	41.144.232.17	37215	TCP
2024-12-22T09:54:40.906992+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45156	131.54.22.125	37215	TCP
2024-12-22T09:54:40.907135+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54942	157.243.44.244	37215	TCP
2024-12-22T09:54:40.939261+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34768	197.58.173.204	37215	TCP
2024-12-22T09:54:41.017638+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48474	41.250.49.135	37215	TCP
2024-12-22T09:54:41.047371+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46540	164.115.182.70	37215	TCP
2024-12-22T09:54:41.062584+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36710	207.115.153.182	37215	TCP
2024-12-22T09:54:41.062951+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54574	103.121.219.225	37215	TCP
2024-12-22T09:54:41.156331+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45192	157.144.162.5	37215	TCP
2024-12-22T09:54:41.156479+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36484	171.174.72.57	37215	TCP
2024-12-22T09:54:41.187794+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45574	41.5.29.7	37215	TCP
2024-12-22T09:54:41.265732+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32820	157.82.121.176	37215	TCP
2024-12-22T09:54:41.281483+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40362	157.1.117.90	37215	TCP
2024-12-22T09:54:41.296951+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38338	197.138.125.200	37215	TCP
2024-12-22T09:54:41.406247+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52528	157.83.176.10	37215	TCP
2024-12-22T09:54:41.430609+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55068	157.123.58.5	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:41.437804+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34206	157.157.167.235	37215	TCP
2024-12-22T09:54:41.688113+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47842	157.16.14.96	37215	TCP
2024-12-22T09:54:41.688147+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38702	157.49.70.213	37215	TCP
2024-12-22T09:54:41.703529+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54134	157.176.36.22	37215	TCP
2024-12-22T09:54:41.703566+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60544	41.13.80.121	37215	TCP
2024-12-22T09:54:41.703654+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56512	197.58.7.230	37215	TCP
2024-12-22T09:54:41.703740+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54470	41.96.151.187	37215	TCP
2024-12-22T09:54:41.703857+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57404	41.242.122.130	37215	TCP
2024-12-22T09:54:41.703887+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57348	197.225.131.194	37215	TCP
2024-12-22T09:54:41.718755+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41318	197.95.9.30	37215	TCP
2024-12-22T09:54:41.718825+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51922	157.143.167.162	37215	TCP
2024-12-22T09:54:41.718918+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38464	197.145.155.50	37215	TCP
2024-12-22T09:54:41.718981+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56102	157.4.23.62	37215	TCP
2024-12-22T09:54:41.719149+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46278	157.77.41.74	37215	TCP
2024-12-22T09:54:41.719215+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35748	157.179.118.157	37215	TCP
2024-12-22T09:54:41.719459+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44704	41.5.6.92	37215	TCP
2024-12-22T09:54:41.719631+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45382	157.176.221.235	37215	TCP
2024-12-22T09:54:41.734663+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52608	197.53.204.94	37215	TCP
2024-12-22T09:54:41.734795+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58526	41.105.3.172	37215	TCP
2024-12-22T09:54:41.734934+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59816	157.136.206.53	37215	TCP
2024-12-22T09:54:41.735065+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35674	197.105.29.188	37215	TCP
2024-12-22T09:54:41.735196+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55748	70.224.88.35	37215	TCP
2024-12-22T09:54:41.735250+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41398	41.134.42.230	37215	TCP
2024-12-22T09:54:41.735464+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34864	41.70.93.7	37215	TCP
2024-12-22T09:54:41.735623+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52808	157.196.42.251	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:41.735663+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47282	95.48.20.248	37215	TCP
2024-12-22T09:54:41.735761+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47936	13.114.93.184	37215	TCP
2024-12-22T09:54:41.736111+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60720	41.100.60.118	37215	TCP
2024-12-22T09:54:41.736493+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45652	193.169.72.207	37215	TCP
2024-12-22T09:54:41.736550+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55458	197.230.15.134	37215	TCP
2024-12-22T09:54:41.736783+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43994	41.1.2.236	37215	TCP
2024-12-22T09:54:41.736928+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41746	197.152.93.63	37215	TCP
2024-12-22T09:54:41.737027+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51782	198.121.91.100	37215	TCP
2024-12-22T09:54:41.737124+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55382	41.217.152.254	37215	TCP
2024-12-22T09:54:41.737316+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52428	197.100.171.57	37215	TCP
2024-12-22T09:54:41.737406+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46058	41.114.75.249	37215	TCP
2024-12-22T09:54:41.737512+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37718	197.109.236.163	37215	TCP
2024-12-22T09:54:41.737618+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57170	41.5.171.252	37215	TCP
2024-12-22T09:54:41.766043+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49922	197.26.20.125	37215	TCP
2024-12-22T09:54:41.766048+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49472	197.238.157.241	37215	TCP
2024-12-22T09:54:41.781506+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55758	157.201.162.7	37215	TCP
2024-12-22T09:54:41.812526+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34936	157.145.67.77	37215	TCP
2024-12-22T09:54:41.843719+0100	2835222	1	A Network Trojan was detected	192.168.2.14	33350	197.195.24.196	37215	TCP
2024-12-22T09:54:41.859363+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38262	157.11.182.118	37215	TCP
2024-12-22T09:54:41.875164+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41376	41.80.131.73	37215	TCP
2024-12-22T09:54:41.875337+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51542	197.92.139.2	37215	TCP
2024-12-22T09:54:41.937719+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57866	157.167.79.27	37215	TCP
2024-12-22T09:54:41.937751+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41548	157.81.173.157	37215	TCP
2024-12-22T09:54:41.937818+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55190	73.34.249.158	37215	TCP
2024-12-22T09:54:41.937988+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48176	157.182.188.210	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:41.938111+0100	2835222	1	A Network Trojan was detected	192.168.2.14	58648	157.75.155.137	37215	TCP
2024-12-22T09:54:41.938181+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42120	41.36.126.225	37215	TCP
2024-12-22T09:54:41.953203+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50676	175.177.109.173	37215	TCP
2024-12-22T09:54:42.031842+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45432	197.61.64.28	37215	TCP
2024-12-22T09:54:42.063089+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35150	197.221.215.197	37215	TCP
2024-12-22T09:54:42.187758+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50512	197.192.96.16	37215	TCP
2024-12-22T09:54:42.203525+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43530	219.29.99.205	37215	TCP
2024-12-22T09:54:42.302974+0100	2835222	1	A Network Trojan was detected	192.168.2.14	54212	157.254.38.151	37215	TCP
2024-12-22T09:54:43.750420+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53640	197.75.16.74	37215	TCP
2024-12-22T09:54:43.750638+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56028	157.59.212.110	37215	TCP
2024-12-22T09:54:43.750704+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35388	41.55.213.127	37215	TCP
2024-12-22T09:54:43.750844+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36592	42.45.214.215	37215	TCP
2024-12-22T09:54:43.765924+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57612	157.47.76.164	37215	TCP
2024-12-22T09:54:43.766059+0100	2835222	1	A Network Trojan was detected	192.168.2.14	36736	76.150.202.9	37215	TCP
2024-12-22T09:54:43.766312+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50898	157.203.117.14	37215	TCP
2024-12-22T09:54:43.766453+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42798	197.215.106.211	37215	TCP
2024-12-22T09:54:43.766756+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49420	197.179.216.8	37215	TCP
2024-12-22T09:54:43.777402+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39296	180.70.144.212	37215	TCP
2024-12-22T09:54:43.781527+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50012	197.32.203.12	37215	TCP
2024-12-22T09:54:43.781605+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55172	197.41.98.107	37215	TCP
2024-12-22T09:54:43.781789+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51426	159.187.203.35	37215	TCP
2024-12-22T09:54:43.782006+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39526	157.30.72.180	37215	TCP
2024-12-22T09:54:43.782007+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41602	41.151.165.203	37215	TCP
2024-12-22T09:54:43.782055+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56316	41.52.171.173	37215	TCP
2024-12-22T09:54:43.782313+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51054	197.22.19.95	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:43.782499+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37634	65.120.78.60	37215	TCP
2024-12-22T09:54:43.782592+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57082	197.22.128.155	37215	TCP
2024-12-22T09:54:43.797123+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39394	41.78.254.164	37215	TCP
2024-12-22T09:54:43.797149+0100	2835222	1	A Network Trojan was detected	192.168.2.14	48274	157.220.79.206	37215	TCP
2024-12-22T09:54:43.797194+0100	2835222	1	A Network Trojan was detected	192.168.2.14	56918	176.139.201.142	37215	TCP
2024-12-22T09:54:43.797261+0100	2835222	1	A Network Trojan was detected	192.168.2.14	41750	157.212.81.222	37215	TCP
2024-12-22T09:54:43.797289+0100	2835222	1	A Network Trojan was detected	192.168.2.14	42710	157.156.34.139	37215	TCP
2024-12-22T09:54:43.812925+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45994	197.226.154.83	37215	TCP
2024-12-22T09:54:43.812991+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59616	197.253.237.105	37215	TCP
2024-12-22T09:54:43.813139+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57636	197.128.28.245	37215	TCP
2024-12-22T09:54:43.813178+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53912	197.231.67.45	37215	TCP
2024-12-22T09:54:43.813241+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43640	157.147.195.237	37215	TCP
2024-12-22T09:54:43.813801+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44282	74.235.31.132	37215	TCP
2024-12-22T09:54:43.860401+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52054	197.126.80.72	37215	TCP
2024-12-22T09:54:43.860510+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45928	46.180.127.93	37215	TCP
2024-12-22T09:54:43.860559+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59736	198.239.207.90	37215	TCP
2024-12-22T09:54:43.891014+0100	2835222	1	A Network Trojan was detected	192.168.2.14	47356	53.216.118.225	37215	TCP
2024-12-22T09:54:43.891083+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35948	44.221.220.67	37215	TCP
2024-12-22T09:54:43.922345+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35908	197.164.231.239	37215	TCP
2024-12-22T09:54:44.062724+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57328	157.11.143.98	37215	TCP
2024-12-22T09:54:44.890852+0100	2835222	1	A Network Trojan was detected	192.168.2.14	49790	41.88.200.41	37215	TCP
2024-12-22T09:54:44.890914+0100	2835222	1	A Network Trojan was detected	192.168.2.14	35208	197.9.237.197	37215	TCP
2024-12-22T09:54:44.906838+0100	2835222	1	A Network Trojan was detected	192.168.2.14	37416	197.94.61.31	37215	TCP
2024-12-22T09:54:44.906922+0100	2835222	1	A Network Trojan was detected	192.168.2.14	34874	41.204.249.60	37215	TCP
2024-12-22T09:54:44.907395+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53502	41.205.209.113	37215	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-22T09:54:44.907663+0100	2835222	1	A Network Trojan was detected	192.168.2.14	53836	40.175.206.61	37215	TCP
2024-12-22T09:54:44.907977+0100	2835222	1	A Network Trojan was detected	192.168.2.14	50062	41.211.176.78	37215	TCP
2024-12-22T09:54:44.908430+0100	2835222	1	A Network Trojan was detected	192.168.2.14	52772	130.228.151.57	37215	TCP
2024-12-22T09:54:44.908490+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40408	197.249.59.36	37215	TCP
2024-12-22T09:54:44.908774+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55912	197.76.228.50	37215	TCP
2024-12-22T09:54:44.908805+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55908	150.62.199.50	37215	TCP
2024-12-22T09:54:44.908900+0100	2835222	1	A Network Trojan was detected	192.168.2.14	45724	197.254.64.229	37215	TCP
2024-12-22T09:54:44.909306+0100	2835222	1	A Network Trojan was detected	192.168.2.14	32824	111.114.109.125	37215	TCP
2024-12-22T09:54:44.909478+0100	2835222	1	A Network Trojan was detected	192.168.2.14	57226	157.34.203.44	37215	TCP
2024-12-22T09:54:44.909614+0100	2835222	1	A Network Trojan was detected	192.168.2.14	51640	197.214.225.35	37215	TCP
2024-12-22T09:54:44.937783+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60742	197.157.158.72	37215	TCP
2024-12-22T09:54:44.937895+0100	2835222	1	A Network Trojan was detected	192.168.2.14	60476	41.4.228.252	37215	TCP
2024-12-22T09:54:44.938005+0100	2835222	1	A Network Trojan was detected	192.168.2.14	59752	201.208.96.148	37215	TCP
2024-12-22T09:54:44.939353+0100	2835222	1	A Network Trojan was detected	192.168.2.14	46184	157.128.230.29	37215	TCP
2024-12-22T09:54:44.939950+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40004	161.23.185.25	37215	TCP
2024-12-22T09:54:44.940376+0100	2835222	1	A Network Trojan was detected	192.168.2.14	44640	197.30.181.2	37215	TCP
2024-12-22T09:54:44.940868+0100	2835222	1	A Network Trojan was detected	192.168.2.14	40262	157.162.189.166	37215	TCP
2024-12-22T09:54:44.941366+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38752	197.39.128.160	37215	TCP
2024-12-22T09:54:44.953178+0100	2835222	1	A Network Trojan was detected	192.168.2.14	55016	197.131.75.140	37215	TCP

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Networking

Suricata IDS alerts for network traffic

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

System Summary

Sample tries to kill multiple processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

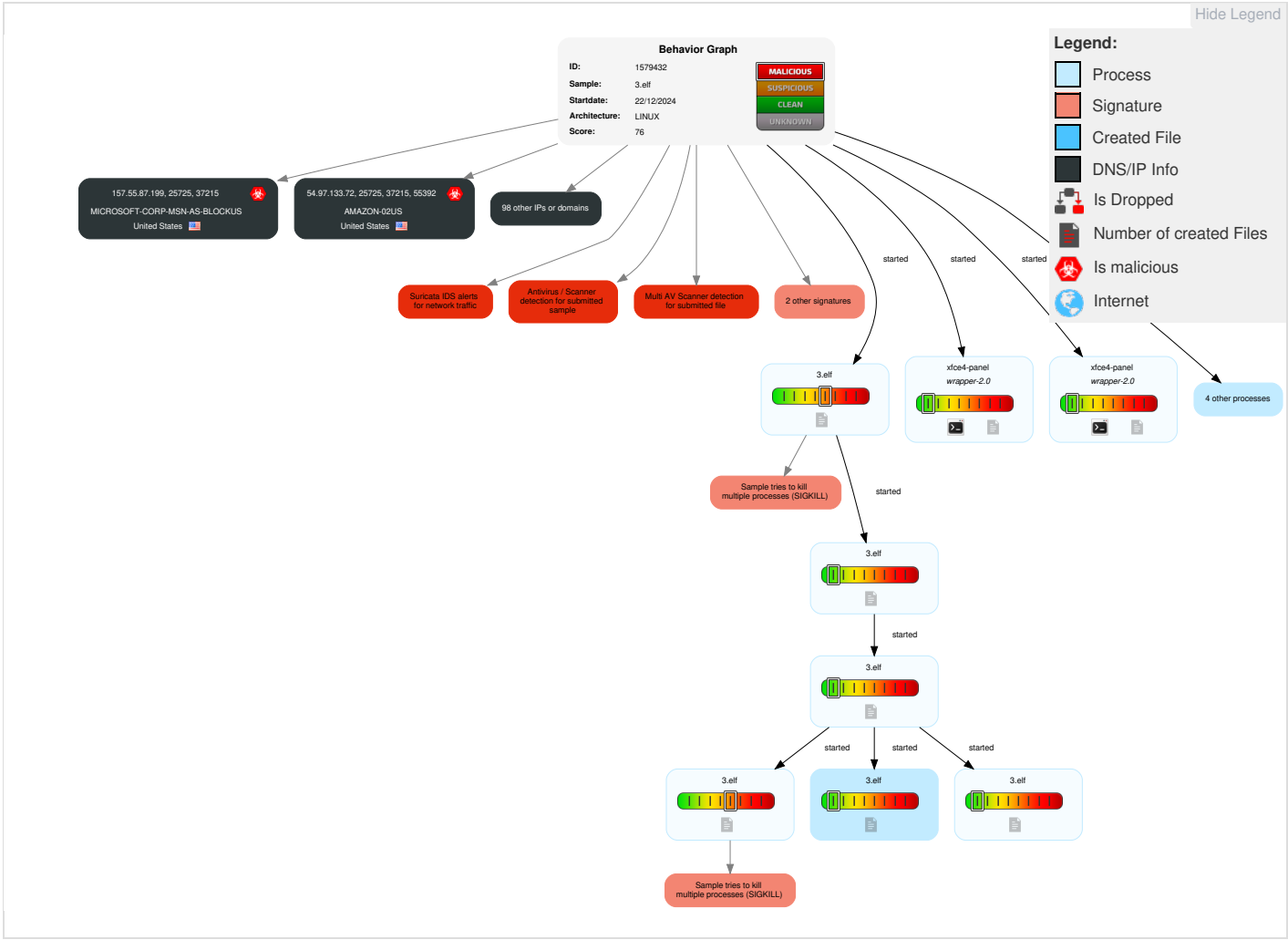
Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 1 Non-Standard Port	Exfiltration Over Other Network Medium	1 Service Stop
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	1 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact

Malware Configuration

No configs have been found

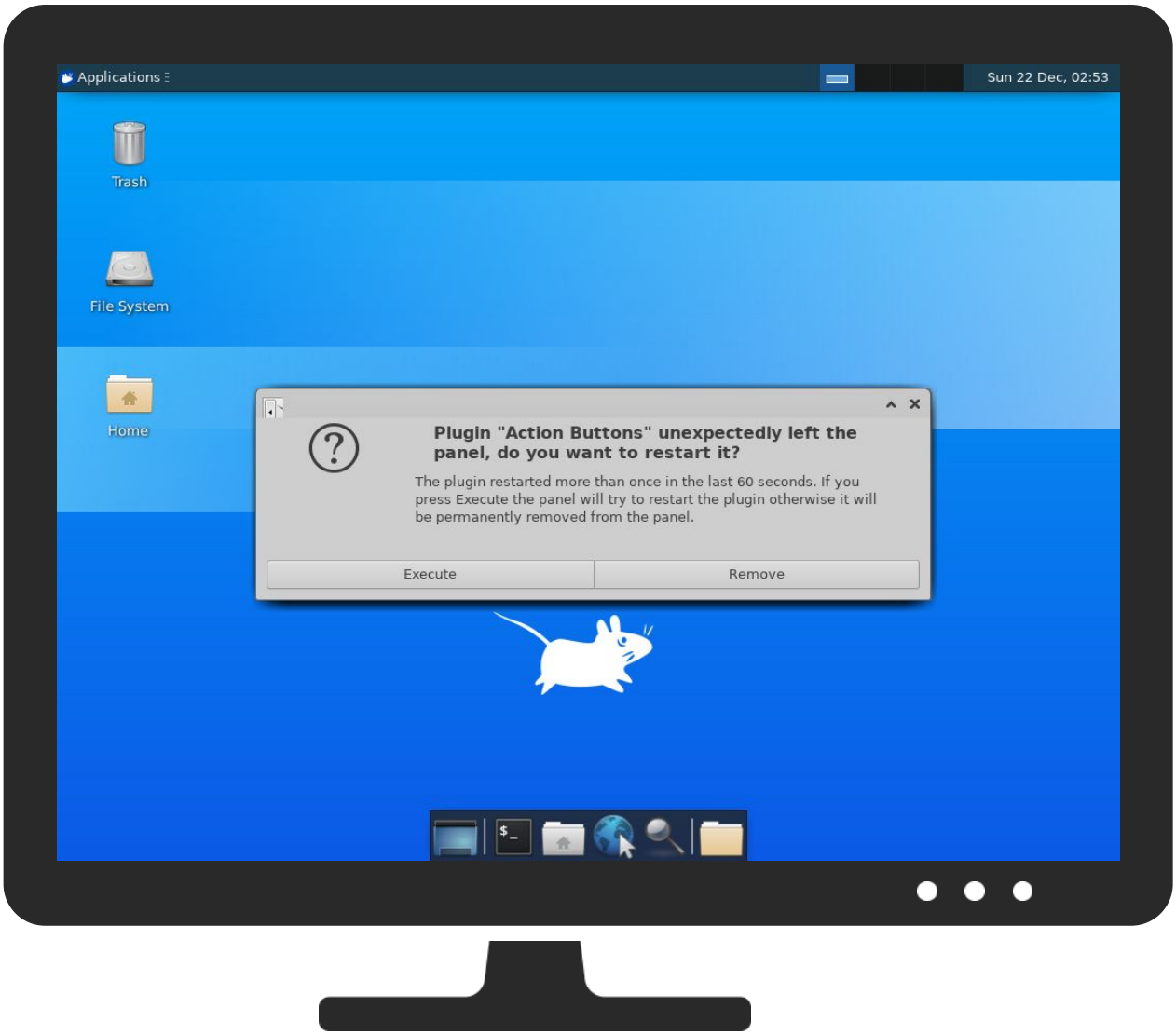
Behavior Graph



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
3.elf	34%	ReversingLabs	Linux.Trojan.Mirai	
3.elf	100%	Avira	EXP/ELF.Mirai.Hua.c	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

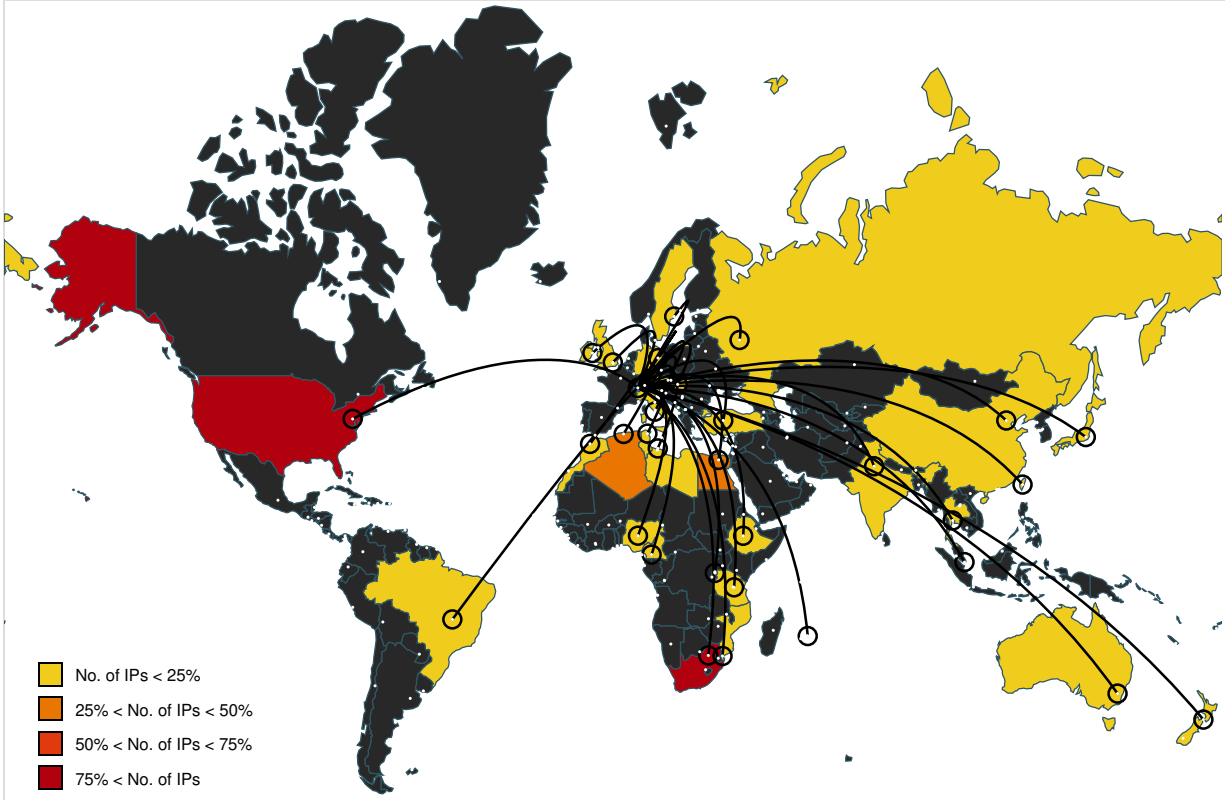
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.89.97.53	unknown	South Africa		10474	OPTINETZA	false
41.253.208.36	unknown	Libyan Arab Jamahiriya		21003	GPTC-ASLY	false
157.151.183.250	unknown	United States		23342	UNITEDLAYERUS	false
203.47.61.114	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
197.87.33.144	unknown	South Africa		10474	OPTINETZA	false
197.154.181.229	unknown	Ethiopia		37133	airtel-tz-asTZ	false
191.216.165.223	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
197.219.152.191	unknown	Mozambique		37342	MOVITELMZ	false
157.183.23.196	unknown	United States		12118	WVUUS	false
157.55.87.199	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
128.126.3.24	unknown	United States		21497	UMC-ASUA	false
157.181.189.191	unknown	Hungary		2012	ELTENETELTENETHU	false
178.241.199.84	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
41.113.157.246	unknown	South Africa		16637	MTNNS-ASZA	false
157.245.170.73	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
157.146.249.221	unknown	United States		719	ELISA-ASHelsinkiFinlandEU	false
157.160.140.240	unknown	United States		22192	SSHENETUS	false
197.133.10.216	unknown	Egypt		24835	RAYA-ASEG	false
41.60.37.75	unknown	Mauritius		30969	ZOL-ASGB	false
208.170.36.114	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
41.21.227.49	unknown	South Africa		36994	Vodacom-VBZA	false
41.172.207.88	unknown	South Africa		36937	Neotel-ASZA	false
197.166.178.10	unknown	Egypt		24863	LINKdotNET-ASEG	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.194.67.88	unknown	Germany		20830	GLOBALAIRNETWORK-ASDE	false
41.166.29.180	unknown	South Africa		36937	Neotel-ASZA	false
197.119.11.229	unknown	Algeria		36947	ALGTEL-ASDZ	false
54.97.133.72	unknown	United States		16509	AMAZON-02US	true
157.134.143.9	unknown	United States		600	OARNET-ASUS	false
157.139.78.199	unknown	United States		20252	JSIWMCUS	false
197.4.212.224	unknown	Tunisia		5438	ATI-TN	false
122.59.185.91	unknown	New Zealand		4771	SPARKNZSparkNewZealandTradingLtdNZ	false
191.248.175.179	unknown	Brazil		18881	TELEFONICABRASILSAB R	false
111.162.29.195	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
197.114.33.151	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.2.68.176	unknown	South Africa		29975	VODACOM-ZA	false
197.73.232.14	unknown	South Africa		16637	MTNNS-ASZA	false
41.122.162.171	unknown	South Africa		16637	MTNNS-ASZA	false
197.96.136.90	unknown	South Africa		3741	ISZA	false
41.96.36.203	unknown	Algeria		36947	ALGTEL-ASDZ	false
162.18.167.11	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
197.185.6.18	unknown	South Africa		37105	NEOLOGY-ASZA	false
157.51.156.220	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
41.128.101.160	unknown	Egypt		24863	LINKdotNET-ASEG	false
202.125.85.228	unknown	Thailand		55451	NBTC-THAI-AS-THOfficeoftheNationalBroadcastingandTH	false
161.33.91.76	unknown	United States		1767	ILIGHT-NETUS	false
197.160.192.211	unknown	Egypt		24863	LINKdotNET-ASEG	false
197.109.134.77	unknown	South Africa		37168	CELL-CZA	false
197.109.183.40	unknown	South Africa		37168	CELL-CZA	false
157.125.42.189	unknown	Sweden		31655	ASN-GAMMATELECOMGB	false
197.87.109.20	unknown	South Africa		10474	OPTINETZA	false
157.112.136.25	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
197.70.12.17	unknown	South Africa		16637	MTNNS-ASZA	false
41.156.87.158	unknown	South Africa		37168	CELL-CZA	false
197.55.123.248	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.119.11.206	unknown	Algeria		36947	ALGTEL-ASDZ	false
98.72.70.85	unknown	United States		7018	ATT-INTERNET4US	false
41.34.56.110	unknown	Egypt		8452	TE-ASTE-ASEG	false
141.201.77.64	unknown	Austria		1109	UNI-SALZBURGUniversityofSalzburgAT	false
197.116.111.99	unknown	Algeria		36947	ALGTEL-ASDZ	false
220.114.179.106	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
197.128.68.36	unknown	Morocco		6713	IAM-ASMA	false
24.153.83.246	unknown	United States		7922	COMCAST-7922US	false
41.242.33.205	unknown	Cameroon		37684	ANGANI-ASKE	false
41.227.31.95	unknown	Tunisia		2609	TN-BB-ASTunisiaBackBoneASTN	false
197.86.143.246	unknown	South Africa		10474	OPTINETZA	false
218.181.62.66	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
137.220.247.57	unknown	Singapore		64050	BCPL-SGBGPNETGlobalASNSG	false
197.224.173.240	unknown	Mauritius		23889	MauritiusTelecomMU	false
157.190.234.182	unknown	Ireland		1213	HEANETIE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.238.132.95	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
41.59.224.149	unknown	Tanzania United Republic of		33765	TTCLDATATZ	false
41.145.83.45	unknown	South Africa		5713	SAIX-NETZA	false
75.82.209.125	unknown	United States		20001	TWC-20001-PACWESTUS	false
41.242.248.243	unknown	South Africa		37105	NEOLOGY-ASZA	false
130.159.16.223	unknown	United Kingdom		786	JANETJiscServicesLimited GB	false
157.222.9.43	unknown	United States		4704	SANNETRakutenMobileInc JP	false
41.203.76.81	unknown	Nigeria		37148	globacom-asNG	false
197.73.220.64	unknown	South Africa		16637	MTNNS-ASZA	false
41.19.31.114	unknown	South Africa		29975	VODACOM-ZA	false
83.171.120.89	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
157.91.133.216	unknown	United States		1767	ILIGHT-NETUS	false
41.106.0.245	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.165.32.17	unknown	Egypt		24863	LINKdotNET-ASEG	false
157.75.91.161	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
98.202.134.231	unknown	United States		7922	COMCAST-7922US	false
41.186.110.99	unknown	Rwanda		36890	MTNRW-ASNRW	false
103.146.47.145	unknown	unknown		139848	SHIPL-AS-APSAFEGUARDHOMEIMPROVEMENTSPTYLTDAU	false
157.229.117.62	unknown	United States		122	UPMC-AS122US	false
87.47.150.191	unknown	Ireland		1213	HEANETIE	false
41.94.199.82	unknown	Mozambique		327700	MoRENetMZ	false
157.35.140.28	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
157.140.67.184	unknown	United Kingdom		786	JANETJiscServicesLimited GB	false
41.129.163.12	unknown	Egypt		24863	LINKdotNET-ASEG	false
157.250.121.37	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	false
157.28.174.134	unknown	Italy		8968	BT-ITALIAIT	false
120.103.236.253	unknown	Taiwan; Republic of China (ROC)		17716	NTU-TWNationalTaiwanUniversityTW	false
92.3.101.179	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
159.44.92.234	unknown	United States		25019	SAUDINETSTC-ASSA	false
197.165.241.185	unknown	Egypt		24863	LINKdotNET-ASEG	false
183.18.84.188	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.0122496486345245
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	3.elf
File size:	75'372 bytes
MD5:	4063c4d9a590ed8aa7611185d5fe548c
SHA1:	0a80aa5fb17e207d54b848a2f091b0137726c4da
SHA256:	909e64490c573de994970cb303bed07463ffa9327f0722f644cd41444ced7de3
SHA512:	4f9db61e0d5d2cbcedc337b6e18e1357e72ef8a4c1b7aca4ee4aa8cc1f65fb17805f54dbdd65c682b8021f49caace2c7b0e1fb8ef88523f70801da89cbd9b3b2
SSDEEP:	1536:ydGGyzkrEFP2DLhwhHFjJ90Zg/haFlPqVuZdbb:UyHklYt9GYYFlPqVWF
TLSH:	77731956F8819742C6D261F7B71E029D37265BA8E2EB7303AD241F1173AEA1F0F27146
File Content Preview:	.ELF...a.....(.....4....$.....4. ...(..... ... ... .I...t-.....Q.td.....-...L."....@.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	74932
Section Header Size:	40
Number of Section Headers:	11
Header String Table Index:	10

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x1039c	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1844c	0x1044c	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x18460	0x10460	0x1358	0x0	0x2	A	0	0	4
.eh_frame	PROGBITS	0x22000	0x12000	0x4	0x0	0x3	WA	0	0	4
.ctors	PROGBITS	0x22004	0x12004	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x2200c	0x1200c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x22018	0x12018	0x454	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x2246c	0x1246c	0x2908	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1246c	0x48	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x117b8	0x117b8	6.1082	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x12000	0x22000	0x22000	0x46c	0x2d74	5.9022	0x6	RW	0x8000		.eh_frame .ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Suricata IDS Alerts

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:09.198274+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41138	197.8.44.33	37215	TCP
2024-12-22T09:54:09.424133+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52976	197.234.184.83	37215	TCP
2024-12-22T09:54:09.693632+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34668	41.175.153.229	37215	TCP
2024-12-22T09:54:12.049891+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54032	192.158.238.237	37215	TCP
2024-12-22T09:54:12.508554+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56430	157.70.215.31	37215	TCP
2024-12-22T09:54:13.530670+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36286	157.25.23.73	37215	TCP
2024-12-22T09:54:14.409934+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58222	94.121.205.148	37215	TCP
2024-12-22T09:54:15.144818+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59856	216.172.184.107	37215	TCP
2024-12-22T09:54:15.598336+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41874	58.125.17.184	37215	TCP
2024-12-22T09:54:15.892277+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56240	197.79.1.153	37215	TCP
2024-12-22T09:54:15.893158+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53936	41.160.23.82	37215	TCP
2024-12-22T09:54:16.667405+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35422	190.111.217.223	37215	TCP
2024-12-22T09:54:17.024085+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33734	197.130.103.71	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:18.647997+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40298	69.55.194.147	37215	TCP
2024-12-22T09:54:19.166930+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48684	103.196.161.173	37215	TCP
2024-12-22T09:54:19.215035+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41512	41.175.103.46	37215	TCP
2024-12-22T09:54:19.241976+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37746	27.7.50.15	37215	TCP
2024-12-22T09:54:19.531696+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58328	197.131.155.200	37215	TCP
2024-12-22T09:54:21.548851+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38556	197.96.88.66	37215	TCP
2024-12-22T09:54:23.465525+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53024	197.130.95.95	37215	TCP
2024-12-22T09:54:24.452706+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46964	157.15.182.30	37215	TCP
2024-12-22T09:54:24.644617+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51724	197.8.125.67	37215	TCP
2024-12-22T09:54:25.428788+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52900	126.55.210.116	37215	TCP
2024-12-22T09:54:25.467008+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59018	126.77.245.205	37215	TCP
2024-12-22T09:54:25.588143+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44832	41.180.59.65	37215	TCP
2024-12-22T09:54:26.359484+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43078	157.97.92.217	37215	TCP
2024-12-22T09:54:26.468614+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33524	157.212.222.149	37215	TCP
2024-12-22T09:54:26.468707+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59662	164.68.151.57	37215	TCP
2024-12-22T09:54:26.468858+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56400	116.253.138.61	37215	TCP
2024-12-22T09:54:26.484259+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53612	41.130.58.215	37215	TCP
2024-12-22T09:54:26.484395+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58442	157.97.136.251	37215	TCP
2024-12-22T09:54:26.484492+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53198	41.23.130.146	37215	TCP
2024-12-22T09:54:26.484660+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43484	157.117.78.8	37215	TCP
2024-12-22T09:54:26.484698+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47192	157.198.199.199	37215	TCP
2024-12-22T09:54:26.484820+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42714	41.16.101.255	37215	TCP
2024-12-22T09:54:26.484916+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49520	148.125.168.63	37215	TCP
2024-12-22T09:54:26.485128+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38284	159.95.198.35	37215	TCP
2024-12-22T09:54:26.485148+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51124	157.8.141.176	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:26.485316+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57594	41.9.170.4	37215	TCP
2024-12-22T09:54:26.485451+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51990	157.240.23.156	37215	TCP
2024-12-22T09:54:26.485512+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33576	210.147.121.17	37215	TCP
2024-12-22T09:54:26.485617+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51190	130.223.41.152	37215	TCP
2024-12-22T09:54:26.485681+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34962	197.201.114.176	37215	TCP
2024-12-22T09:54:26.485828+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46698	197.236.36.156	37215	TCP
2024-12-22T09:54:26.485947+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50116	41.147.22.216	37215	TCP
2024-12-22T09:54:26.486032+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56216	41.36.58.35	37215	TCP
2024-12-22T09:54:26.486197+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59296	157.155.234.87	37215	TCP
2024-12-22T09:54:26.486467+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55494	74.177.63.156	37215	TCP
2024-12-22T09:54:26.499760+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38822	143.93.223.56	37215	TCP
2024-12-22T09:54:26.499850+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47276	41.136.164.85	37215	TCP
2024-12-22T09:54:26.499886+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51860	41.119.52.109	37215	TCP
2024-12-22T09:54:26.515575+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40556	41.134.226.53	37215	TCP
2024-12-22T09:54:26.515671+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39404	197.105.18.62	37215	TCP
2024-12-22T09:54:26.515681+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52286	197.79.252.108	37215	TCP
2024-12-22T09:54:26.562577+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49730	41.5.185.41	37215	TCP
2024-12-22T09:54:26.562611+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43662	197.123.70.200	37215	TCP
2024-12-22T09:54:26.562678+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36492	104.184.158.66	37215	TCP
2024-12-22T09:54:26.804303+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44470	222.145.114.194	37215	TCP
2024-12-22T09:54:27.249688+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56528	157.108.252.165	37215	TCP
2024-12-22T09:54:27.265280+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54616	41.183.31.203	37215	TCP
2024-12-22T09:54:27.265382+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37300	157.51.247.114	37215	TCP
2024-12-22T09:54:27.265567+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50552	195.218.231.50	37215	TCP
2024-12-22T09:54:27.281007+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51102	41.157.137.219	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:27.281089+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50080	157.58.177.30	37215	TCP
2024-12-22T09:54:27.281179+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36758	197.39.181.173	37215	TCP
2024-12-22T09:54:27.284992+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39470	157.90.244.87	37215	TCP
2024-12-22T09:54:27.296595+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42430	41.181.52.151	37215	TCP
2024-12-22T09:54:27.296719+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43932	197.154.0.129	37215	TCP
2024-12-22T09:54:27.296803+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46382	197.60.78.44	37215	TCP
2024-12-22T09:54:27.296919+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49888	41.186.240.129	37215	TCP
2024-12-22T09:54:27.297062+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38582	197.214.187.242	37215	TCP
2024-12-22T09:54:27.297191+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39996	197.142.123.239	37215	TCP
2024-12-22T09:54:27.515348+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41764	41.148.226.129	37215	TCP
2024-12-22T09:54:27.515475+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39870	157.87.159.28	37215	TCP
2024-12-22T09:54:27.515538+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51764	157.97.73.39	37215	TCP
2024-12-22T09:54:27.515603+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33868	157.47.242.235	37215	TCP
2024-12-22T09:54:27.515718+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57778	193.254.103.145	37215	TCP
2024-12-22T09:54:27.515824+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53248	41.20.137.108	37215	TCP
2024-12-22T09:54:27.530880+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38358	197.88.175.54	37215	TCP
2024-12-22T09:54:27.531040+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40840	41.205.6.37	37215	TCP
2024-12-22T09:54:27.531080+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43546	197.200.93.131	37215	TCP
2024-12-22T09:54:27.531182+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51288	41.76.174.231	37215	TCP
2024-12-22T09:54:27.531286+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55108	157.187.30.13	37215	TCP
2024-12-22T09:54:27.531445+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58572	41.208.156.218	37215	TCP
2024-12-22T09:54:27.531487+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37052	157.181.120.184	37215	TCP
2024-12-22T09:54:27.546921+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56626	157.53.229.73	37215	TCP
2024-12-22T09:54:27.562397+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47908	157.24.149.224	37215	TCP
2024-12-22T09:54:27.562406+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40498	197.137.175.56	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:27.577897+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46468	197.106.58.1	37215	TCP
2024-12-22T09:54:27.594280+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52028	41.67.7.71	37215	TCP
2024-12-22T09:54:27.609341+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47694	197.39.211.11	37215	TCP
2024-12-22T09:54:27.625012+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53048	157.205.43.230	37215	TCP
2024-12-22T09:54:27.640434+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48660	157.206.148.101	37215	TCP
2024-12-22T09:54:27.640536+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37286	157.20.144.151	37215	TCP
2024-12-22T09:54:27.640694+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39788	197.96.37.76	37215	TCP
2024-12-22T09:54:27.656122+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43910	41.81.4.100	37215	TCP
2024-12-22T09:54:27.656244+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41746	197.45.32.190	37215	TCP
2024-12-22T09:54:27.656430+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48762	157.127.74.230	37215	TCP
2024-12-22T09:54:27.656567+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38284	197.208.96.236	37215	TCP
2024-12-22T09:54:27.671649+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35826	157.214.180.28	37215	TCP
2024-12-22T09:54:27.687392+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51684	197.103.59.243	37215	TCP
2024-12-22T09:54:27.687449+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34216	157.61.126.107	37215	TCP
2024-12-22T09:54:27.760185+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38310	41.175.14.253	37215	TCP
2024-12-22T09:54:28.656454+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58064	41.150.101.178	37215	TCP
2024-12-22T09:54:28.671846+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33554	157.177.163.177	37215	TCP
2024-12-22T09:54:28.671866+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33654	222.56.33.107	37215	TCP
2024-12-22T09:54:28.672018+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55362	197.84.170.215	37215	TCP
2024-12-22T09:54:28.672111+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45852	157.18.29.81	37215	TCP
2024-12-22T09:54:28.672254+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40980	41.104.210.63	37215	TCP
2024-12-22T09:54:28.672334+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37734	47.150.218.100	37215	TCP
2024-12-22T09:54:28.672362+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52354	197.26.203.165	37215	TCP
2024-12-22T09:54:28.687414+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35774	41.86.192.23	37215	TCP
2024-12-22T09:54:28.687531+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39266	41.39.157.52	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:28.687621+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38804	75.215.82.126	37215	TCP
2024-12-22T09:54:28.687766+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37810	91.244.234.3	37215	TCP
2024-12-22T09:54:28.687895+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44282	186.2.18.215	37215	TCP
2024-12-22T09:54:28.687993+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44468	75.161.123.10	37215	TCP
2024-12-22T09:54:28.688167+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42888	157.76.79.65	37215	TCP
2024-12-22T09:54:28.688297+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51804	157.96.157.112	37215	TCP
2024-12-22T09:54:28.688509+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48012	183.180.168.157	37215	TCP
2024-12-22T09:54:28.688681+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41056	41.35.181.9	37215	TCP
2024-12-22T09:54:28.688815+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48120	41.229.147.16	37215	TCP
2024-12-22T09:54:28.688880+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39148	41.137.74.188	37215	TCP
2024-12-22T09:54:28.689045+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57532	41.129.24.92	37215	TCP
2024-12-22T09:54:28.689178+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44172	157.71.136.134	37215	TCP
2024-12-22T09:54:28.689297+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59784	157.22.61.101	37215	TCP
2024-12-22T09:54:28.689383+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50216	197.162.97.194	37215	TCP
2024-12-22T09:54:28.689482+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60148	41.13.114.85	37215	TCP
2024-12-22T09:54:28.689571+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41462	157.86.245.102	37215	TCP
2024-12-22T09:54:28.689773+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43182	157.29.49.0	37215	TCP
2024-12-22T09:54:28.689903+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58958	183.218.229.124	37215	TCP
2024-12-22T09:54:28.690024+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49738	197.28.6.169	37215	TCP
2024-12-22T09:54:28.690103+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58866	81.216.206.52	37215	TCP
2024-12-22T09:54:28.690334+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50870	101.177.12.75	37215	TCP
2024-12-22T09:54:28.690468+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54784	143.92.250.1	37215	TCP
2024-12-22T09:54:28.690550+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45934	160.52.86.56	37215	TCP
2024-12-22T09:54:28.690709+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52708	197.126.129.166	37215	TCP
2024-12-22T09:54:28.718616+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57478	189.183.109.113	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:28.718710+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53274	41.216.98.247	37215	TCP
2024-12-22T09:54:28.718844+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51258	197.68.125.160	37215	TCP
2024-12-22T09:54:28.718971+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51622	203.7.240.130	37215	TCP
2024-12-22T09:54:28.719110+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41486	197.190.246.243	37215	TCP
2024-12-22T09:54:28.719233+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41946	130.194.13.32	37215	TCP
2024-12-22T09:54:28.719391+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39568	43.71.255.139	37215	TCP
2024-12-22T09:54:28.719471+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42154	157.207.215.253	37215	TCP
2024-12-22T09:54:28.719539+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46432	41.26.89.205	37215	TCP
2024-12-22T09:54:28.719735+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33636	57.31.9.67	37215	TCP
2024-12-22T09:54:28.796638+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48992	157.87.198.107	37215	TCP
2024-12-22T09:54:28.803435+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44106	197.181.105.208	37215	TCP
2024-12-22T09:54:28.803593+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58306	197.177.131.26	37215	TCP
2024-12-22T09:54:28.812185+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41806	41.208.1.52	37215	TCP
2024-12-22T09:54:28.812348+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53082	197.204.163.228	37215	TCP
2024-12-22T09:54:28.812482+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35452	41.1.52.53	37215	TCP
2024-12-22T09:54:28.812651+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49722	157.227.220.23	37215	TCP
2024-12-22T09:54:28.812761+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42718	180.46.37.61	37215	TCP
2024-12-22T09:54:28.812898+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33738	197.25.193.152	37215	TCP
2024-12-22T09:54:28.813061+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44080	197.20.125.221	37215	TCP
2024-12-22T09:54:28.813285+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45824	157.78.246.143	37215	TCP
2024-12-22T09:54:28.813404+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50000	157.6.135.22	37215	TCP
2024-12-22T09:54:28.813522+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40112	197.108.155.249	37215	TCP
2024-12-22T09:54:29.531244+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41616	41.140.24.85	37215	TCP
2024-12-22T09:54:29.531460+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59000	195.227.69.17	37215	TCP
2024-12-22T09:54:29.531556+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44370	41.86.110.125	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:29.531634+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46438	41.164.5.41	37215	TCP
2024-12-22T09:54:29.546900+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36414	197.209.246.114	37215	TCP
2024-12-22T09:54:29.547009+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33652	20.87.214.216	37215	TCP
2024-12-22T09:54:29.547100+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39410	41.118.44.139	37215	TCP
2024-12-22T09:54:29.547162+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47780	168.226.133.129	37215	TCP
2024-12-22T09:54:29.562396+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60388	184.244.251.232	37215	TCP
2024-12-22T09:54:29.562522+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55328	41.242.233.42	37215	TCP
2024-12-22T09:54:29.562649+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50104	157.121.228.177	37215	TCP
2024-12-22T09:54:29.562672+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57802	197.25.158.160	37215	TCP
2024-12-22T09:54:29.562833+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50140	81.191.160.152	37215	TCP
2024-12-22T09:54:29.562884+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60824	157.154.202.117	37215	TCP
2024-12-22T09:54:29.563090+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44990	41.45.211.90	37215	TCP
2024-12-22T09:54:29.563186+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56576	41.252.119.148	37215	TCP
2024-12-22T09:54:29.563392+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58454	157.26.100.2	37215	TCP
2024-12-22T09:54:29.563494+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41492	197.9.32.122	37215	TCP
2024-12-22T09:54:29.563641+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51436	52.220.227.249	37215	TCP
2024-12-22T09:54:29.577984+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53904	197.239.140.210	37215	TCP
2024-12-22T09:54:29.578146+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53458	75.190.174.103	37215	TCP
2024-12-22T09:54:29.578176+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53442	197.223.10.64	37215	TCP
2024-12-22T09:54:29.578382+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33274	41.224.49.149	37215	TCP
2024-12-22T09:54:29.578488+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59672	41.143.89.233	37215	TCP
2024-12-22T09:54:29.578582+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37694	41.237.42.179	37215	TCP
2024-12-22T09:54:29.578726+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39808	89.76.195.178	37215	TCP
2024-12-22T09:54:29.578824+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56808	107.58.133.196	37215	TCP
2024-12-22T09:54:29.578972+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43310	65.213.58.156	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:29.579271+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36278	43.92.198.168	37215	TCP
2024-12-22T09:54:29.579456+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44468	157.90.220.190	37215	TCP
2024-12-22T09:54:29.579557+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45278	41.50.182.238	37215	TCP
2024-12-22T09:54:29.579716+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47496	20.0.88.186	37215	TCP
2024-12-22T09:54:29.579876+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47266	93.233.231.169	37215	TCP
2024-12-22T09:54:29.580026+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41616	197.206.51.156	37215	TCP
2024-12-22T09:54:29.580139+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39282	116.0.252.48	37215	TCP
2024-12-22T09:54:29.580304+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57974	157.93.31.153	37215	TCP
2024-12-22T09:54:29.580431+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57254	157.145.4.173	37215	TCP
2024-12-22T09:54:29.580549+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40574	41.98.245.14	37215	TCP
2024-12-22T09:54:29.580585+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34448	157.35.55.24	37215	TCP
2024-12-22T09:54:29.593506+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51096	41.26.23.169	37215	TCP
2024-12-22T09:54:29.593635+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56134	157.239.244.189	37215	TCP
2024-12-22T09:54:29.593743+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33286	157.208.40.95	37215	TCP
2024-12-22T09:54:29.593920+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39406	197.85.171.173	37215	TCP
2024-12-22T09:54:29.594045+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58590	157.214.105.119	37215	TCP
2024-12-22T09:54:29.594184+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49812	197.223.203.65	37215	TCP
2024-12-22T09:54:29.594302+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37464	157.242.148.55	37215	TCP
2024-12-22T09:54:29.594554+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43080	76.112.145.202	37215	TCP
2024-12-22T09:54:29.594598+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60716	197.211.128.1	37215	TCP
2024-12-22T09:54:29.594720+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52196	53.204.222.67	37215	TCP
2024-12-22T09:54:29.640511+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36534	197.240.71.169	37215	TCP
2024-12-22T09:54:29.687671+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34314	197.182.114.58	37215	TCP
2024-12-22T09:54:29.703116+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33148	41.139.238.45	37215	TCP
2024-12-22T09:54:29.703241+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57692	41.242.29.160	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:29.781309+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59678	157.222.40.29	37215	TCP
2024-12-22T09:54:29.796611+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52646	122.251.144.61	37215	TCP
2024-12-22T09:54:29.796691+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41678	41.203.136.73	37215	TCP
2024-12-22T09:54:29.812639+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35826	197.67.145.250	37215	TCP
2024-12-22T09:54:29.812692+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58084	157.212.245.162	37215	TCP
2024-12-22T09:54:29.812846+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55200	41.69.126.24	37215	TCP
2024-12-22T09:54:29.812918+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32768	41.13.58.48	37215	TCP
2024-12-22T09:54:29.813002+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36324	41.99.200.127	37215	TCP
2024-12-22T09:54:29.813111+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34536	197.52.102.205	37215	TCP
2024-12-22T09:54:29.813273+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41802	157.93.20.165	37215	TCP
2024-12-22T09:54:29.813403+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53648	41.128.81.128	37215	TCP
2024-12-22T09:54:29.828060+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53744	157.2.95.174	37215	TCP
2024-12-22T09:54:30.587239+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36432	157.161.255.5	37215	TCP
2024-12-22T09:54:30.687355+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54006	157.118.148.134	37215	TCP
2024-12-22T09:54:30.687531+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58292	84.64.32.109	37215	TCP
2024-12-22T09:54:30.687647+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42320	157.97.24.174	37215	TCP
2024-12-22T09:54:30.687762+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56294	157.40.208.249	37215	TCP
2024-12-22T09:54:30.687922+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57180	197.44.131.108	37215	TCP
2024-12-22T09:54:30.688085+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45338	41.249.54.244	37215	TCP
2024-12-22T09:54:30.688208+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34004	143.229.146.137	37215	TCP
2024-12-22T09:54:30.688329+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59036	41.33.229.30	37215	TCP
2024-12-22T09:54:30.688432+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60140	41.85.52.93	37215	TCP
2024-12-22T09:54:30.688562+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45392	157.204.104.209	37215	TCP
2024-12-22T09:54:30.688785+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51416	197.233.151.209	37215	TCP
2024-12-22T09:54:30.688887+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40412	197.190.120.144	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:30.688985+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53996	197.202.20.213	37215	TCP
2024-12-22T09:54:30.689164+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48004	157.169.78.81	37215	TCP
2024-12-22T09:54:30.689427+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56508	197.98.73.12	37215	TCP
2024-12-22T09:54:30.689542+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37298	41.88.234.15	37215	TCP
2024-12-22T09:54:30.689643+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38932	88.82.33.192	37215	TCP
2024-12-22T09:54:30.689789+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59402	197.182.144.123	37215	TCP
2024-12-22T09:54:30.689912+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50058	163.226.218.0	37215	TCP
2024-12-22T09:54:30.690013+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43848	143.158.252.131	37215	TCP
2024-12-22T09:54:30.690122+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41368	197.38.250.83	37215	TCP
2024-12-22T09:54:30.690254+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56498	197.183.57.234	37215	TCP
2024-12-22T09:54:30.690365+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47434	157.58.173.13	37215	TCP
2024-12-22T09:54:30.690498+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43176	157.120.146.98	37215	TCP
2024-12-22T09:54:30.690608+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60354	157.151.3.153	37215	TCP
2024-12-22T09:54:30.690737+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52748	189.93.52.121	37215	TCP
2024-12-22T09:54:30.690851+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40594	168.180.70.181	37215	TCP
2024-12-22T09:54:30.690933+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40446	138.239.183.100	37215	TCP
2024-12-22T09:54:30.691035+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37660	41.9.165.26	37215	TCP
2024-12-22T09:54:30.691155+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40848	157.169.35.141	37215	TCP
2024-12-22T09:54:30.691346+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53346	140.181.132.148	37215	TCP
2024-12-22T09:54:30.691496+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43524	197.166.126.43	37215	TCP
2024-12-22T09:54:30.691661+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35388	157.69.32.146	37215	TCP
2024-12-22T09:54:30.691927+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45318	209.178.86.248	37215	TCP
2024-12-22T09:54:30.692088+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45386	90.233.74.9	37215	TCP
2024-12-22T09:54:30.692292+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52372	41.133.219.10	37215	TCP
2024-12-22T09:54:30.718622+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60842	77.118.183.164	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:30.725521+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45406	41.47.186.85	37215	TCP
2024-12-22T09:54:30.734338+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58566	197.58.78.221	37215	TCP
2024-12-22T09:54:30.734409+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44084	197.175.159.24	37215	TCP
2024-12-22T09:54:30.734437+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55952	80.9.142.201	37215	TCP
2024-12-22T09:54:30.734530+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51776	41.125.231.243	37215	TCP
2024-12-22T09:54:30.734566+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42412	197.228.1.0	37215	TCP
2024-12-22T09:54:30.734671+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58556	197.242.32.201	37215	TCP
2024-12-22T09:54:30.734781+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53816	197.152.156.114	37215	TCP
2024-12-22T09:54:30.828469+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47394	41.234.174.75	37215	TCP
2024-12-22T09:54:30.828469+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35472	157.63.231.146	37215	TCP
2024-12-22T09:54:30.828478+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48166	197.77.93.138	37215	TCP
2024-12-22T09:54:30.914370+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51882	197.215.218.231	37215	TCP
2024-12-22T09:54:31.859373+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52930	157.244.148.110	37215	TCP
2024-12-22T09:54:31.859431+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41762	60.180.176.199	37215	TCP
2024-12-22T09:54:31.859478+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58856	17.18.223.255	37215	TCP
2024-12-22T09:54:31.984473+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51492	187.94.63.249	37215	TCP
2024-12-22T09:54:31.984499+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38688	41.151.220.159	37215	TCP
2024-12-22T09:54:31.990847+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57510	41.41.203.128	37215	TCP
2024-12-22T09:54:31.990889+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55622	197.155.35.161	37215	TCP
2024-12-22T09:54:31.990905+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34978	197.173.55.207	37215	TCP
2024-12-22T09:54:31.991013+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33094	157.148.167.181	37215	TCP
2024-12-22T09:54:31.991103+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55162	41.59.216.125	37215	TCP
2024-12-22T09:54:31.991227+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49834	95.255.215.200	37215	TCP
2024-12-22T09:54:31.991403+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42394	116.86.106.134	37215	TCP
2024-12-22T09:54:31.991495+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55826	197.34.99.195	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:32.021627+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56946	157.250.111.37	37215	TCP
2024-12-22T09:54:32.021663+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58632	157.27.171.67	37215	TCP
2024-12-22T09:54:32.032812+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36776	197.41.197.99	37215	TCP
2024-12-22T09:54:32.828265+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46016	36.72.0.118	37215	TCP
2024-12-22T09:54:32.843770+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55392	54.97.133.72	37215	TCP
2024-12-22T09:54:32.843969+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39180	197.46.45.137	37215	TCP
2024-12-22T09:54:32.843969+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46014	41.2.218.69	37215	TCP
2024-12-22T09:54:32.843973+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53174	197.162.33.29	37215	TCP
2024-12-22T09:54:32.844068+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34862	157.148.224.133	37215	TCP
2024-12-22T09:54:32.844287+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37678	73.55.9.63	37215	TCP
2024-12-22T09:54:32.844366+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56056	197.28.96.46	37215	TCP
2024-12-22T09:54:32.844395+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58432	143.119.80.45	37215	TCP
2024-12-22T09:54:32.844500+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46356	157.3.91.94	37215	TCP
2024-12-22T09:54:32.859480+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50730	157.93.80.87	37215	TCP
2024-12-22T09:54:32.859619+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46710	170.117.89.88	37215	TCP
2024-12-22T09:54:32.859774+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45618	197.253.21.39	37215	TCP
2024-12-22T09:54:32.859908+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60840	106.250.214.38	37215	TCP
2024-12-22T09:54:32.860021+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48806	41.202.189.221	37215	TCP
2024-12-22T09:54:32.860070+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43146	197.213.32.2	37215	TCP
2024-12-22T09:54:32.860260+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55828	157.225.103.240	37215	TCP
2024-12-22T09:54:32.860359+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50490	197.116.79.106	37215	TCP
2024-12-22T09:54:32.860423+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41396	197.63.230.149	37215	TCP
2024-12-22T09:54:32.860451+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41690	191.155.104.32	37215	TCP
2024-12-22T09:54:32.860571+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53520	157.107.65.19	37215	TCP
2024-12-22T09:54:32.860601+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34560	197.167.68.215	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:32.860747+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36072	41.145.214.123	37215	TCP
2024-12-22T09:54:32.860777+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54786	190.16.226.175	37215	TCP
2024-12-22T09:54:32.860800+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36590	41.101.2.255	37215	TCP
2024-12-22T09:54:32.860899+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48230	41.193.245.135	37215	TCP
2024-12-22T09:54:32.860971+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48210	83.183.25.243	37215	TCP
2024-12-22T09:54:32.874960+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48408	157.88.5.62	37215	TCP
2024-12-22T09:54:32.875164+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38932	197.66.58.69	37215	TCP
2024-12-22T09:54:32.875170+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41704	41.51.160.41	37215	TCP
2024-12-22T09:54:32.875396+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51620	45.43.197.24	37215	TCP
2024-12-22T09:54:32.875547+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41832	112.55.197.163	37215	TCP
2024-12-22T09:54:32.875616+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34720	197.217.156.54	37215	TCP
2024-12-22T09:54:32.875684+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33414	157.109.168.173	37215	TCP
2024-12-22T09:54:32.875884+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37114	197.176.211.202	37215	TCP
2024-12-22T09:54:32.875972+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48166	155.245.5.80	37215	TCP
2024-12-22T09:54:32.876250+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46826	197.95.102.234	37215	TCP
2024-12-22T09:54:32.876312+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55928	57.120.164.60	37215	TCP
2024-12-22T09:54:32.876431+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41866	41.92.103.130	37215	TCP
2024-12-22T09:54:32.876489+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58048	41.126.50.239	37215	TCP
2024-12-22T09:54:32.876585+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42378	197.121.204.226	37215	TCP
2024-12-22T09:54:32.876866+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43684	41.6.113.145	37215	TCP
2024-12-22T09:54:32.890670+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56794	71.2.188.186	37215	TCP
2024-12-22T09:54:32.890835+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55332	41.82.231.215	37215	TCP
2024-12-22T09:54:32.890857+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54034	41.11.153.105	37215	TCP
2024-12-22T09:54:32.891103+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45006	41.84.131.80	37215	TCP
2024-12-22T09:54:32.891131+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36278	197.105.81.129	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:32.891258+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43190	157.251.189.201	37215	TCP
2024-12-22T09:54:32.891410+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41894	157.149.116.62	37215	TCP
2024-12-22T09:54:32.891437+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49926	188.206.56.235	37215	TCP
2024-12-22T09:54:32.891545+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32868	20.195.212.83	37215	TCP
2024-12-22T09:54:32.891691+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41234	157.178.37.222	37215	TCP
2024-12-22T09:54:32.891795+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46184	150.175.198.56	37215	TCP
2024-12-22T09:54:32.891833+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58888	38.156.221.8	37215	TCP
2024-12-22T09:54:32.938229+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60832	157.141.198.60	37215	TCP
2024-12-22T09:54:32.953310+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58606	197.160.57.98	37215	TCP
2024-12-22T09:54:32.953389+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55084	157.63.107.13	37215	TCP
2024-12-22T09:54:32.954294+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57402	220.230.234.118	37215	TCP
2024-12-22T09:54:32.954493+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47176	41.157.65.27	37215	TCP
2024-12-22T09:54:32.968624+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55934	197.194.90.129	37215	TCP
2024-12-22T09:54:32.968739+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54362	197.167.129.134	37215	TCP
2024-12-22T09:54:32.968804+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47328	125.253.30.17	37215	TCP
2024-12-22T09:54:32.968931+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49418	41.152.28.21	37215	TCP
2024-12-22T09:54:32.968977+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51462	155.217.169.105	37215	TCP
2024-12-22T09:54:32.969129+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42098	223.83.135.244	37215	TCP
2024-12-22T09:54:32.969259+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60706	157.166.215.229	37215	TCP
2024-12-22T09:54:32.969358+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55768	157.209.140.43	37215	TCP
2024-12-22T09:54:32.969580+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48272	37.208.8.186	37215	TCP
2024-12-22T09:54:32.969709+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53078	9.228.193.2	37215	TCP
2024-12-22T09:54:32.969774+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41936	41.65.120.27	37215	TCP
2024-12-22T09:54:32.969871+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53060	157.20.66.146	37215	TCP
2024-12-22T09:54:32.970004+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57708	54.168.88.251	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:32.970308+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53236	197.91.182.226	37215	TCP
2024-12-22T09:54:32.970575+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49552	184.237.113.21	37215	TCP
2024-12-22T09:54:32.984427+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55250	41.10.130.191	37215	TCP
2024-12-22T09:54:32.984659+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38168	197.45.224.37	37215	TCP
2024-12-22T09:54:33.078336+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37172	157.216.217.226	37215	TCP
2024-12-22T09:54:33.078364+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41832	197.115.42.51	37215	TCP
2024-12-22T09:54:33.093956+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32870	197.125.168.173	37215	TCP
2024-12-22T09:54:33.094170+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33600	200.66.53.98	37215	TCP
2024-12-22T09:54:33.094228+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36718	41.66.225.84	37215	TCP
2024-12-22T09:54:33.094230+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34114	197.241.94.41	37215	TCP
2024-12-22T09:54:33.187441+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44512	157.116.180.215	37215	TCP
2024-12-22T09:54:33.203127+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53390	41.139.174.37	37215	TCP
2024-12-22T09:54:33.203280+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46020	157.70.68.103	37215	TCP
2024-12-22T09:54:33.203405+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56278	109.29.181.227	37215	TCP
2024-12-22T09:54:33.203518+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42624	197.21.60.249	37215	TCP
2024-12-22T09:54:33.218701+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35974	158.214.140.26	37215	TCP
2024-12-22T09:54:33.219040+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53498	197.166.76.145	37215	TCP
2024-12-22T09:54:33.219040+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52848	197.19.131.195	37215	TCP
2024-12-22T09:54:33.219064+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39866	157.96.78.80	37215	TCP
2024-12-22T09:54:33.219155+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52814	134.190.208.237	37215	TCP
2024-12-22T09:54:33.219244+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40376	197.136.111.231	37215	TCP
2024-12-22T09:54:33.219424+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35594	197.117.121.5	37215	TCP
2024-12-22T09:54:33.219461+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60434	157.150.148.102	37215	TCP
2024-12-22T09:54:33.219598+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36000	41.131.206.191	37215	TCP
2024-12-22T09:54:33.855356+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36138	41.71.163.235	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:34.096792+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54774	154.114.19.92	37215	TCP
2024-12-22T09:54:34.187779+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57900	41.45.230.95	37215	TCP
2024-12-22T09:54:34.203112+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50960	157.228.237.76	37215	TCP
2024-12-22T09:54:34.203197+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51444	90.42.183.197	37215	TCP
2024-12-22T09:54:34.203204+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52186	41.130.91.234	37215	TCP
2024-12-22T09:54:34.218775+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38266	197.176.208.92	37215	TCP
2024-12-22T09:54:35.015586+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43786	197.137.182.27	37215	TCP
2024-12-22T09:54:35.015730+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59722	73.194.247.19	37215	TCP
2024-12-22T09:54:35.015964+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55320	41.12.222.242	37215	TCP
2024-12-22T09:54:35.016142+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49178	157.184.72.196	37215	TCP
2024-12-22T09:54:35.016287+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54802	23.133.172.170	37215	TCP
2024-12-22T09:54:35.016474+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44552	157.198.235.115	37215	TCP
2024-12-22T09:54:35.016645+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55510	197.143.141.156	37215	TCP
2024-12-22T09:54:35.016912+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57136	157.116.237.232	37215	TCP
2024-12-22T09:54:35.017046+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54298	197.209.12.236	37215	TCP
2024-12-22T09:54:35.017178+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59456	41.77.5.100	37215	TCP
2024-12-22T09:54:35.017295+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41812	96.41.99.37	37215	TCP
2024-12-22T09:54:35.017443+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43884	157.78.16.247	37215	TCP
2024-12-22T09:54:35.017556+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60412	197.126.8.237	37215	TCP
2024-12-22T09:54:35.017597+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42400	197.196.204.10	37215	TCP
2024-12-22T09:54:35.017640+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38806	41.223.59.176	37215	TCP
2024-12-22T09:54:35.017801+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37090	157.229.225.51	37215	TCP
2024-12-22T09:54:35.017927+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55070	41.19.239.36	37215	TCP
2024-12-22T09:54:35.018066+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59812	66.27.238.142	37215	TCP
2024-12-22T09:54:35.018184+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57164	157.119.229.47	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:35.018300+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37172	157.105.228.121	37215	TCP
2024-12-22T09:54:35.018381+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36022	41.55.243.171	37215	TCP
2024-12-22T09:54:35.018559+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48992	157.219.217.229	37215	TCP
2024-12-22T09:54:35.018664+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43212	157.217.70.147	37215	TCP
2024-12-22T09:54:35.018836+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51116	157.231.177.245	37215	TCP
2024-12-22T09:54:35.018891+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46944	157.254.42.112	37215	TCP
2024-12-22T09:54:35.031246+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38300	157.19.62.171	37215	TCP
2024-12-22T09:54:35.031323+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47582	140.185.220.66	37215	TCP
2024-12-22T09:54:35.031425+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49466	197.149.147.88	37215	TCP
2024-12-22T09:54:35.031610+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45672	41.76.99.195	37215	TCP
2024-12-22T09:54:35.031739+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48098	199.236.111.157	37215	TCP
2024-12-22T09:54:35.062453+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60920	157.49.241.166	37215	TCP
2024-12-22T09:54:35.062579+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35224	157.92.30.133	37215	TCP
2024-12-22T09:54:35.062710+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32856	197.120.129.255	37215	TCP
2024-12-22T09:54:35.062800+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37374	41.172.79.137	37215	TCP
2024-12-22T09:54:35.062825+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51306	157.13.225.74	37215	TCP
2024-12-22T09:54:35.062959+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43046	157.102.98.62	37215	TCP
2024-12-22T09:54:35.063089+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58038	197.128.198.210	37215	TCP
2024-12-22T09:54:35.063254+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41724	41.133.133.181	37215	TCP
2024-12-22T09:54:35.063390+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53058	41.48.174.32	37215	TCP
2024-12-22T09:54:35.063485+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57492	223.18.187.215	37215	TCP
2024-12-22T09:54:35.063646+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34370	157.210.177.65	37215	TCP
2024-12-22T09:54:35.063727+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33028	197.142.151.217	37215	TCP
2024-12-22T09:54:35.063890+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38872	197.207.124.159	37215	TCP
2024-12-22T09:54:35.063998+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51876	41.26.61.237	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:35.064095+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58486	138.226.78.54	37215	TCP
2024-12-22T09:54:35.064171+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44510	41.76.76.62	37215	TCP
2024-12-22T09:54:35.064298+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40212	41.241.124.45	37215	TCP
2024-12-22T09:54:35.064515+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37240	157.12.60.128	37215	TCP
2024-12-22T09:54:35.064636+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38952	123.109.145.174	37215	TCP
2024-12-22T09:54:35.064699+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53140	206.133.93.70	37215	TCP
2024-12-22T09:54:35.064924+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60042	157.181.139.67	37215	TCP
2024-12-22T09:54:35.065019+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41618	197.211.166.214	37215	TCP
2024-12-22T09:54:35.065132+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40336	43.19.29.173	37215	TCP
2024-12-22T09:54:35.065224+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32922	197.61.225.161	37215	TCP
2024-12-22T09:54:35.065275+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60282	197.236.125.148	37215	TCP
2024-12-22T09:54:35.065341+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47882	157.146.13.88	37215	TCP
2024-12-22T09:54:35.065490+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38366	74.210.170.36	37215	TCP
2024-12-22T09:54:35.065631+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49784	157.159.28.214	37215	TCP
2024-12-22T09:54:35.065673+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33332	25.39.229.133	37215	TCP
2024-12-22T09:54:35.065743+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58808	190.186.151.60	37215	TCP
2024-12-22T09:54:35.065846+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53186	157.165.13.125	37215	TCP
2024-12-22T09:54:35.065940+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43734	157.77.6.112	37215	TCP
2024-12-22T09:54:35.066019+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55906	197.58.253.179	37215	TCP
2024-12-22T09:54:35.066128+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58914	197.123.83.143	37215	TCP
2024-12-22T09:54:35.066161+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42826	41.46.120.193	37215	TCP
2024-12-22T09:54:35.066263+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43170	217.175.106.75	37215	TCP
2024-12-22T09:54:35.066306+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44410	188.133.186.239	37215	TCP
2024-12-22T09:54:35.068028+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45784	197.131.153.162	37215	TCP
2024-12-22T09:54:35.156005+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60208	141.162.146.172	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:35.156122+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57812	157.93.235.58	37215	TCP
2024-12-22T09:54:35.156237+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52840	216.211.132.202	37215	TCP
2024-12-22T09:54:35.187462+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59038	93.171.13.0	37215	TCP
2024-12-22T09:54:35.187605+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50006	152.15.160.101	37215	TCP
2024-12-22T09:54:35.187728+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59948	174.56.71.142	37215	TCP
2024-12-22T09:54:35.265694+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36636	197.123.110.112	37215	TCP
2024-12-22T09:54:35.265840+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56106	197.70.237.1	37215	TCP
2024-12-22T09:54:35.281200+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37088	197.210.136.112	37215	TCP
2024-12-22T09:54:35.281291+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39872	157.248.254.241	37215	TCP
2024-12-22T09:54:35.281447+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51520	157.207.218.36	37215	TCP
2024-12-22T09:54:35.296777+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35244	41.168.233.196	37215	TCP
2024-12-22T09:54:36.156510+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36214	84.172.12.182	37215	TCP
2024-12-22T09:54:36.156588+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49024	197.5.193.200	37215	TCP
2024-12-22T09:54:36.156598+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41388	113.244.68.174	37215	TCP
2024-12-22T09:54:36.156609+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43710	41.57.139.31	37215	TCP
2024-12-22T09:54:36.156696+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51100	157.180.238.38	37215	TCP
2024-12-22T09:54:36.156790+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32938	41.129.63.233	37215	TCP
2024-12-22T09:54:36.156910+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57892	157.225.139.208	37215	TCP
2024-12-22T09:54:36.157136+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60154	157.140.131.136	37215	TCP
2024-12-22T09:54:36.157280+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49096	157.46.7.49	37215	TCP
2024-12-22T09:54:36.171799+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41052	157.216.75.179	37215	TCP
2024-12-22T09:54:36.171999+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50546	197.79.17.131	37215	TCP
2024-12-22T09:54:36.172022+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43388	20.230.182.145	37215	TCP
2024-12-22T09:54:36.172110+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49258	41.202.129.65	37215	TCP
2024-12-22T09:54:36.172290+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49382	197.199.243.49	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:36.172457+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48706	220.54.189.215	37215	TCP
2024-12-22T09:54:36.172540+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41986	74.211.127.9	37215	TCP
2024-12-22T09:54:36.172643+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51224	197.19.114.32	37215	TCP
2024-12-22T09:54:36.172727+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56368	41.144.99.10	37215	TCP
2024-12-22T09:54:36.172822+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43682	41.143.239.184	37215	TCP
2024-12-22T09:54:36.172983+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47290	197.103.143.48	37215	TCP
2024-12-22T09:54:36.173108+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47150	197.129.74.251	37215	TCP
2024-12-22T09:54:36.173317+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55010	197.115.106.116	37215	TCP
2024-12-22T09:54:36.173443+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58072	157.31.163.165	37215	TCP
2024-12-22T09:54:36.173554+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43322	41.206.177.175	37215	TCP
2024-12-22T09:54:36.173675+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45814	213.133.46.194	37215	TCP
2024-12-22T09:54:36.173776+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33538	157.149.125.151	37215	TCP
2024-12-22T09:54:36.173850+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54306	123.74.154.250	37215	TCP
2024-12-22T09:54:36.173934+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58932	197.88.247.123	37215	TCP
2024-12-22T09:54:36.174006+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53750	197.95.53.45	37215	TCP
2024-12-22T09:54:36.174096+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33504	41.42.42.128	37215	TCP
2024-12-22T09:54:36.174193+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59326	157.66.120.23	37215	TCP
2024-12-22T09:54:36.174285+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57692	150.23.156.8	37215	TCP
2024-12-22T09:54:36.174395+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55000	197.181.46.251	37215	TCP
2024-12-22T09:54:36.174515+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40602	89.143.85.248	37215	TCP
2024-12-22T09:54:36.174628+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43628	157.226.248.132	37215	TCP
2024-12-22T09:54:36.174707+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38710	157.52.98.77	37215	TCP
2024-12-22T09:54:36.174783+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54394	41.130.109.164	37215	TCP
2024-12-22T09:54:36.174874+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58316	157.33.176.94	37215	TCP
2024-12-22T09:54:36.174956+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59478	157.146.236.76	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:36.175050+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55054	80.128.9.77	37215	TCP
2024-12-22T09:54:36.175463+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46392	157.30.251.95	37215	TCP
2024-12-22T09:54:36.175554+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44140	157.99.47.57	37215	TCP
2024-12-22T09:54:36.175587+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49564	197.56.223.242	37215	TCP
2024-12-22T09:54:36.175717+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58066	41.104.94.89	37215	TCP
2024-12-22T09:54:36.187303+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57112	41.121.204.244	37215	TCP
2024-12-22T09:54:36.187412+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49216	197.187.64.94	37215	TCP
2024-12-22T09:54:36.187558+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54736	157.113.254.70	37215	TCP
2024-12-22T09:54:36.187670+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48778	157.39.63.65	37215	TCP
2024-12-22T09:54:36.187791+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42164	207.42.247.33	37215	TCP
2024-12-22T09:54:36.187931+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47330	41.69.134.82	37215	TCP
2024-12-22T09:54:36.187976+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45224	197.3.134.64	37215	TCP
2024-12-22T09:54:36.202948+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56592	157.148.151.222	37215	TCP
2024-12-22T09:54:36.203144+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33106	157.50.158.175	37215	TCP
2024-12-22T09:54:36.203160+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37342	197.85.116.249	37215	TCP
2024-12-22T09:54:36.203335+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44408	68.175.86.152	37215	TCP
2024-12-22T09:54:36.203344+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45638	157.156.242.16	37215	TCP
2024-12-22T09:54:36.203460+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58870	197.241.145.155	37215	TCP
2024-12-22T09:54:36.203534+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46448	146.198.245.6	37215	TCP
2024-12-22T09:54:36.203615+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51296	197.52.110.114	37215	TCP
2024-12-22T09:54:36.203707+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53462	45.126.101.33	37215	TCP
2024-12-22T09:54:36.203993+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42106	157.11.3.59	37215	TCP
2024-12-22T09:54:36.204122+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35778	41.126.91.241	37215	TCP
2024-12-22T09:54:36.204151+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50852	197.201.157.89	37215	TCP
2024-12-22T09:54:36.204225+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51098	197.141.192.167	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:36.218700+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53992	157.85.207.129	37215	TCP
2024-12-22T09:54:36.218947+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48232	41.58.181.104	37215	TCP
2024-12-22T09:54:36.218956+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54074	43.107.99.245	37215	TCP
2024-12-22T09:54:36.219043+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38812	197.0.111.119	37215	TCP
2024-12-22T09:54:36.219138+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45988	197.55.134.216	37215	TCP
2024-12-22T09:54:36.219298+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40062	96.92.59.70	37215	TCP
2024-12-22T09:54:36.219353+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35640	197.158.250.182	37215	TCP
2024-12-22T09:54:36.219456+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41324	157.215.27.64	37215	TCP
2024-12-22T09:54:36.219556+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48732	85.53.135.10	37215	TCP
2024-12-22T09:54:36.219658+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52920	41.138.111.184	37215	TCP
2024-12-22T09:54:36.219759+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44534	157.28.54.168	37215	TCP
2024-12-22T09:54:36.220098+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37598	157.237.6.220	37215	TCP
2024-12-22T09:54:36.220270+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33984	41.144.133.216	37215	TCP
2024-12-22T09:54:36.220298+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59166	137.105.247.184	37215	TCP
2024-12-22T09:54:36.220399+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54760	157.154.79.80	37215	TCP
2024-12-22T09:54:36.220528+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53696	157.98.253.164	37215	TCP
2024-12-22T09:54:36.220631+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41120	193.85.48.73	37215	TCP
2024-12-22T09:54:36.220732+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37602	157.141.157.83	37215	TCP
2024-12-22T09:54:36.220842+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59800	41.23.147.191	37215	TCP
2024-12-22T09:54:36.220933+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33532	93.177.177.212	37215	TCP
2024-12-22T09:54:36.221031+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37348	157.156.45.70	37215	TCP
2024-12-22T09:54:36.221123+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52508	157.244.111.60	37215	TCP
2024-12-22T09:54:36.221232+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49396	41.26.240.145	37215	TCP
2024-12-22T09:54:36.221259+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55602	157.113.226.117	37215	TCP
2024-12-22T09:54:36.221408+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38818	197.9.181.58	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:36.221507+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36956	157.88.169.191	37215	TCP
2024-12-22T09:54:36.234215+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49522	41.160.148.227	37215	TCP
2024-12-22T09:54:36.234337+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54926	157.192.108.52	37215	TCP
2024-12-22T09:54:36.234477+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44946	41.44.4.244	37215	TCP
2024-12-22T09:54:36.234570+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51342	157.128.85.66	37215	TCP
2024-12-22T09:54:36.296856+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45388	41.17.162.79	37215	TCP
2024-12-22T09:54:36.406209+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48336	41.65.254.41	37215	TCP
2024-12-22T09:54:36.406281+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41132	157.119.10.131	37215	TCP
2024-12-22T09:54:36.406413+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32808	126.228.223.35	37215	TCP
2024-12-22T09:54:36.406457+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50430	207.186.61.146	37215	TCP
2024-12-22T09:54:36.437518+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37044	41.183.49.72	37215	TCP
2024-12-22T09:54:36.437657+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35988	205.46.48.39	37215	TCP
2024-12-22T09:54:37.456492+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54630	219.85.237.133	37215	TCP
2024-12-22T09:54:38.187922+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52576	197.10.9.135	37215	TCP
2024-12-22T09:54:38.187922+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40022	157.220.98.251	37215	TCP
2024-12-22T09:54:38.203238+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46546	157.217.224.59	37215	TCP
2024-12-22T09:54:38.203413+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45006	197.29.215.218	37215	TCP
2024-12-22T09:54:38.218818+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48668	157.174.103.141	37215	TCP
2024-12-22T09:54:38.218818+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39128	196.34.166.220	37215	TCP
2024-12-22T09:54:38.328193+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37516	211.252.175.92	37215	TCP
2024-12-22T09:54:38.343986+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34272	197.222.205.230	37215	TCP
2024-12-22T09:54:38.343990+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43668	197.43.103.180	37215	TCP
2024-12-22T09:54:38.343996+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41732	197.104.116.144	37215	TCP
2024-12-22T09:54:38.344102+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56522	197.162.42.120	37215	TCP
2024-12-22T09:54:38.344255+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38344	172.245.106.1	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.344382+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56352	41.172.13.39	37215	TCP
2024-12-22T09:54:38.344509+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37956	197.60.60.16	37215	TCP
2024-12-22T09:54:38.344691+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48682	157.37.50.166	37215	TCP
2024-12-22T09:54:38.344972+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47942	41.43.13.26	37215	TCP
2024-12-22T09:54:38.345096+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34058	157.94.171.73	37215	TCP
2024-12-22T09:54:38.345164+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48076	119.106.145.205	37215	TCP
2024-12-22T09:54:38.345344+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44658	41.82.149.155	37215	TCP
2024-12-22T09:54:38.356089+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50986	197.238.212.204	37215	TCP
2024-12-22T09:54:38.356151+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37376	197.38.185.22	37215	TCP
2024-12-22T09:54:38.356202+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36858	41.50.67.148	37215	TCP
2024-12-22T09:54:38.356341+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37230	64.47.250.112	37215	TCP
2024-12-22T09:54:38.359191+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40634	41.231.51.216	37215	TCP
2024-12-22T09:54:38.359357+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52076	157.170.143.128	37215	TCP
2024-12-22T09:54:38.359471+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41150	197.7.18.61	37215	TCP
2024-12-22T09:54:38.359588+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38800	41.188.73.193	37215	TCP
2024-12-22T09:54:38.359709+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51928	41.214.193.173	37215	TCP
2024-12-22T09:54:38.359872+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46412	137.44.18.179	37215	TCP
2024-12-22T09:54:38.359956+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36760	83.41.195.201	37215	TCP
2024-12-22T09:54:38.360106+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55416	197.40.207.53	37215	TCP
2024-12-22T09:54:38.360273+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35638	197.241.179.130	37215	TCP
2024-12-22T09:54:38.360584+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53736	41.217.103.0	37215	TCP
2024-12-22T09:54:38.360742+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55954	157.190.234.237	37215	TCP
2024-12-22T09:54:38.360877+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36814	197.8.58.127	37215	TCP
2024-12-22T09:54:38.361026+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54190	40.120.46.26	37215	TCP
2024-12-22T09:54:38.361147+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58608	157.89.191.234	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.361182+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42218	175.183.217.123	37215	TCP
2024-12-22T09:54:38.361303+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47478	86.219.171.106	37215	TCP
2024-12-22T09:54:38.361395+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57998	204.18.4.163	37215	TCP
2024-12-22T09:54:38.361588+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43748	197.239.208.39	37215	TCP
2024-12-22T09:54:38.361734+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40698	197.230.213.167	37215	TCP
2024-12-22T09:54:38.361865+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32814	46.99.172.115	37215	TCP
2024-12-22T09:54:38.361925+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38974	41.32.177.151	37215	TCP
2024-12-22T09:54:38.362084+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34670	157.182.252.124	37215	TCP
2024-12-22T09:54:38.362188+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44092	122.91.199.102	37215	TCP
2024-12-22T09:54:38.362358+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41566	40.46.160.129	37215	TCP
2024-12-22T09:54:38.362411+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51520	167.228.57.6	37215	TCP
2024-12-22T09:54:38.362501+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52202	41.54.171.10	37215	TCP
2024-12-22T09:54:38.362563+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57418	148.189.102.87	37215	TCP
2024-12-22T09:54:38.362671+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60630	157.82.149.3	37215	TCP
2024-12-22T09:54:38.362926+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50850	197.87.191.59	37215	TCP
2024-12-22T09:54:38.363093+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47032	58.45.181.81	37215	TCP
2024-12-22T09:54:38.363145+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46110	41.188.16.55	37215	TCP
2024-12-22T09:54:38.363250+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39302	157.102.9.38	37215	TCP
2024-12-22T09:54:38.390554+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50206	206.72.181.115	37215	TCP
2024-12-22T09:54:38.429019+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38054	41.9.137.61	37215	TCP
2024-12-22T09:54:38.429056+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56418	41.37.164.157	37215	TCP
2024-12-22T09:54:38.429086+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38128	205.171.75.214	37215	TCP
2024-12-22T09:54:38.437320+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47382	41.139.112.115	37215	TCP
2024-12-22T09:54:38.437425+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42898	157.119.150.238	37215	TCP
2024-12-22T09:54:38.437595+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33174	46.103.23.179	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.437668+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53776	41.203.206.27	37215	TCP
2024-12-22T09:54:38.437911+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36566	197.86.86.40	37215	TCP
2024-12-22T09:54:38.438150+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58878	192.12.52.5	37215	TCP
2024-12-22T09:54:38.438267+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35468	41.161.30.26	37215	TCP
2024-12-22T09:54:38.438299+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51360	1.69.55.80	37215	TCP
2024-12-22T09:54:38.438454+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50712	197.107.36.10	37215	TCP
2024-12-22T09:54:38.438583+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42370	41.72.129.236	37215	TCP
2024-12-22T09:54:38.438708+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37964	41.31.143.8	37215	TCP
2024-12-22T09:54:38.438820+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58442	41.43.110.134	37215	TCP
2024-12-22T09:54:38.438933+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56912	197.88.252.222	37215	TCP
2024-12-22T09:54:38.439013+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49854	197.185.171.75	37215	TCP
2024-12-22T09:54:38.439081+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59214	152.224.192.122	37215	TCP
2024-12-22T09:54:38.439226+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59162	41.185.22.109	37215	TCP
2024-12-22T09:54:38.439366+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33748	197.114.162.167	37215	TCP
2024-12-22T09:54:38.439465+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46360	201.75.163.101	37215	TCP
2024-12-22T09:54:38.439588+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59692	197.145.57.186	37215	TCP
2024-12-22T09:54:38.439605+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56250	134.71.74.92	37215	TCP
2024-12-22T09:54:38.439754+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37418	41.9.170.50	37215	TCP
2024-12-22T09:54:38.439879+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40418	157.100.62.149	37215	TCP
2024-12-22T09:54:38.439959+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48536	157.47.139.221	37215	TCP
2024-12-22T09:54:38.440018+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37880	157.61.121.161	37215	TCP
2024-12-22T09:54:38.440122+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35668	157.202.180.151	37215	TCP
2024-12-22T09:54:38.440406+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45732	157.236.88.63	37215	TCP
2024-12-22T09:54:38.440527+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35824	41.212.130.32	37215	TCP
2024-12-22T09:54:38.440698+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34240	197.214.202.165	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.453535+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51004	120.75.13.116	37215	TCP
2024-12-22T09:54:38.453721+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49668	157.111.225.114	37215	TCP
2024-12-22T09:54:38.453903+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38526	41.164.167.173	37215	TCP
2024-12-22T09:54:38.453958+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42218	197.176.188.167	37215	TCP
2024-12-22T09:54:38.454059+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34212	157.206.216.143	37215	TCP
2024-12-22T09:54:38.454128+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54264	157.85.229.12	37215	TCP
2024-12-22T09:54:38.454241+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49808	197.82.91.205	37215	TCP
2024-12-22T09:54:38.454362+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44526	197.211.40.53	37215	TCP
2024-12-22T09:54:38.468762+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40686	206.212.28.113	37215	TCP
2024-12-22T09:54:38.468995+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55886	41.198.77.226	37215	TCP
2024-12-22T09:54:38.469003+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53742	98.3.110.46	37215	TCP
2024-12-22T09:54:38.469136+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52638	157.143.19.134	37215	TCP
2024-12-22T09:54:38.469233+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41116	157.199.173.146	37215	TCP
2024-12-22T09:54:38.469302+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50728	157.230.219.236	37215	TCP
2024-12-22T09:54:38.469390+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47832	197.244.78.206	37215	TCP
2024-12-22T09:54:38.469508+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44542	157.23.136.155	37215	TCP
2024-12-22T09:54:38.469612+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47896	41.116.123.134	37215	TCP
2024-12-22T09:54:38.469770+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48872	41.126.14.168	37215	TCP
2024-12-22T09:54:38.469840+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38988	197.88.171.122	37215	TCP
2024-12-22T09:54:38.469920+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53636	157.9.52.41	37215	TCP
2024-12-22T09:54:38.470045+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56054	197.33.142.56	37215	TCP
2024-12-22T09:54:38.470138+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45336	197.112.91.61	37215	TCP
2024-12-22T09:54:38.470299+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46262	65.206.81.30	37215	TCP
2024-12-22T09:54:38.470403+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48860	41.83.51.17	37215	TCP
2024-12-22T09:54:38.470431+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39802	9.3.82.165	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.470530+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33276	41.105.147.157	37215	TCP
2024-12-22T09:54:38.470632+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50138	157.41.197.149	37215	TCP
2024-12-22T09:54:38.484396+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48950	157.178.87.150	37215	TCP
2024-12-22T09:54:38.484518+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43568	41.6.225.193	37215	TCP
2024-12-22T09:54:38.484642+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39782	197.213.36.103	37215	TCP
2024-12-22T09:54:38.484759+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35618	157.221.20.255	37215	TCP
2024-12-22T09:54:38.484854+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54922	41.135.226.124	37215	TCP
2024-12-22T09:54:38.484952+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36756	157.119.24.24	37215	TCP
2024-12-22T09:54:38.485081+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59386	41.176.205.103	37215	TCP
2024-12-22T09:54:38.485323+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40930	197.123.199.156	37215	TCP
2024-12-22T09:54:38.485437+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47040	41.1.23.104	37215	TCP
2024-12-22T09:54:38.485551+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39024	62.66.90.167	37215	TCP
2024-12-22T09:54:38.485674+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39680	41.58.157.153	37215	TCP
2024-12-22T09:54:38.485792+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44958	197.88.108.124	37215	TCP
2024-12-22T09:54:38.485978+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58512	197.209.137.164	37215	TCP
2024-12-22T09:54:38.486095+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42062	157.89.253.41	37215	TCP
2024-12-22T09:54:38.486218+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41806	202.154.54.63	37215	TCP
2024-12-22T09:54:38.486334+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36532	157.35.124.193	37215	TCP
2024-12-22T09:54:38.486462+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40484	197.60.151.237	37215	TCP
2024-12-22T09:54:38.486577+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38496	147.130.1.100	37215	TCP
2024-12-22T09:54:38.486623+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33882	197.15.81.135	37215	TCP
2024-12-22T09:54:38.486721+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41916	157.252.209.81	37215	TCP
2024-12-22T09:54:38.486822+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40752	2.107.168.123	37215	TCP
2024-12-22T09:54:38.486949+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37964	197.192.126.208	37215	TCP
2024-12-22T09:54:38.487042+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37362	166.208.171.185	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.487123+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58122	101.53.29.54	37215	TCP
2024-12-22T09:54:38.487273+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45678	41.195.133.181	37215	TCP
2024-12-22T09:54:38.487520+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58470	72.77.130.129	37215	TCP
2024-12-22T09:54:38.487622+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39124	41.28.1.80	37215	TCP
2024-12-22T09:54:38.487731+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46102	223.60.55.208	37215	TCP
2024-12-22T09:54:38.487888+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55380	197.155.18.234	37215	TCP
2024-12-22T09:54:38.487978+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50520	41.82.37.74	37215	TCP
2024-12-22T09:54:38.488079+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56632	185.190.246.117	37215	TCP
2024-12-22T09:54:38.488213+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55510	65.29.142.24	37215	TCP
2024-12-22T09:54:38.488333+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59662	41.96.144.190	37215	TCP
2024-12-22T09:54:38.488425+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36102	197.28.112.45	37215	TCP
2024-12-22T09:54:38.488522+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54712	41.80.63.229	37215	TCP
2024-12-22T09:54:38.488615+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43050	157.113.86.82	37215	TCP
2024-12-22T09:54:38.488682+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34920	157.117.2.25	37215	TCP
2024-12-22T09:54:38.488801+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57094	157.96.66.232	37215	TCP
2024-12-22T09:54:38.488916+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57754	157.148.174.120	37215	TCP
2024-12-22T09:54:38.488979+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42834	197.10.229.114	37215	TCP
2024-12-22T09:54:38.489085+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52612	157.72.118.234	37215	TCP
2024-12-22T09:54:38.489208+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35226	197.233.125.34	37215	TCP
2024-12-22T09:54:38.489275+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43832	41.153.102.92	37215	TCP
2024-12-22T09:54:38.489503+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45544	157.91.8.252	37215	TCP
2024-12-22T09:54:38.489541+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41764	41.14.84.14	37215	TCP
2024-12-22T09:54:38.489633+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51958	41.167.189.101	37215	TCP
2024-12-22T09:54:38.489744+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58380	13.90.196.182	37215	TCP
2024-12-22T09:54:38.489872+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60500	157.112.136.25	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.489954+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35046	197.181.68.93	37215	TCP
2024-12-22T09:54:38.490028+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55922	93.134.187.80	37215	TCP
2024-12-22T09:54:38.490116+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54288	197.246.129.216	37215	TCP
2024-12-22T09:54:38.490230+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54276	197.48.55.68	37215	TCP
2024-12-22T09:54:38.490259+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40286	157.175.245.169	37215	TCP
2024-12-22T09:54:38.490463+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48182	197.12.78.27	37215	TCP
2024-12-22T09:54:38.490574+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58876	197.244.248.146	37215	TCP
2024-12-22T09:54:38.490631+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60800	27.123.199.8	37215	TCP
2024-12-22T09:54:38.490693+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44004	192.162.61.139	37215	TCP
2024-12-22T09:54:38.490787+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55206	177.154.80.115	37215	TCP
2024-12-22T09:54:38.490893+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36358	197.170.64.62	37215	TCP
2024-12-22T09:54:38.490925+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34886	157.242.210.47	37215	TCP
2024-12-22T09:54:38.491018+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59862	197.201.55.176	37215	TCP
2024-12-22T09:54:38.491126+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37832	61.32.33.34	37215	TCP
2024-12-22T09:54:38.491237+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55272	197.243.158.108	37215	TCP
2024-12-22T09:54:38.491348+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36004	197.149.2.90	37215	TCP
2024-12-22T09:54:38.491410+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54562	41.213.61.71	37215	TCP
2024-12-22T09:54:38.491531+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47926	216.62.186.126	37215	TCP
2024-12-22T09:54:38.491649+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33712	41.170.6.36	37215	TCP
2024-12-22T09:54:38.491721+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45092	157.2.90.13	37215	TCP
2024-12-22T09:54:38.491842+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34662	41.88.74.242	37215	TCP
2024-12-22T09:54:38.492015+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38300	41.4.80.228	37215	TCP
2024-12-22T09:54:38.492141+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54664	41.46.35.48	37215	TCP
2024-12-22T09:54:38.492277+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56548	197.40.17.236	37215	TCP
2024-12-22T09:54:38.492381+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48452	157.190.146.59	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.492463+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42300	197.26.228.143	37215	TCP
2024-12-22T09:54:38.492506+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49442	41.231.143.124	37215	TCP
2024-12-22T09:54:38.492605+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41692	41.129.79.156	37215	TCP
2024-12-22T09:54:38.492697+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51752	157.76.202.27	37215	TCP
2024-12-22T09:54:38.492793+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41094	157.243.142.130	37215	TCP
2024-12-22T09:54:38.492895+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41712	1.99.134.121	37215	TCP
2024-12-22T09:54:38.493073+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39838	41.144.213.56	37215	TCP
2024-12-22T09:54:38.493190+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51692	197.221.43.146	37215	TCP
2024-12-22T09:54:38.493224+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54296	41.35.55.253	37215	TCP
2024-12-22T09:54:38.493290+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60062	197.31.74.2	37215	TCP
2024-12-22T09:54:38.493376+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59262	157.140.99.31	37215	TCP
2024-12-22T09:54:38.493606+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57564	157.243.3.139	37215	TCP
2024-12-22T09:54:38.493699+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44964	197.146.185.193	37215	TCP
2024-12-22T09:54:38.493781+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41146	41.14.115.66	37215	TCP
2024-12-22T09:54:38.493888+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52038	41.71.41.176	37215	TCP
2024-12-22T09:54:38.493998+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34270	102.93.162.142	37215	TCP
2024-12-22T09:54:38.494069+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55844	41.207.190.237	37215	TCP
2024-12-22T09:54:38.494146+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54770	157.209.99.126	37215	TCP
2024-12-22T09:54:38.494251+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36960	197.245.24.42	37215	TCP
2024-12-22T09:54:38.494421+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55092	157.219.220.114	37215	TCP
2024-12-22T09:54:38.494545+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37358	213.25.62.71	37215	TCP
2024-12-22T09:54:38.494576+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33120	197.105.75.172	37215	TCP
2024-12-22T09:54:38.494669+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56986	197.52.126.211	37215	TCP
2024-12-22T09:54:38.495104+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43364	41.9.105.19	37215	TCP
2024-12-22T09:54:38.495249+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54992	41.10.198.166	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.495379+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46252	157.3.99.90	37215	TCP
2024-12-22T09:54:38.495411+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39340	41.107.251.32	37215	TCP
2024-12-22T09:54:38.495497+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33988	218.131.124.172	37215	TCP
2024-12-22T09:54:38.495630+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46728	96.225.10.71	37215	TCP
2024-12-22T09:54:38.495741+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58840	41.237.39.152	37215	TCP
2024-12-22T09:54:38.495900+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34540	89.107.191.235	37215	TCP
2024-12-22T09:54:38.495986+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42430	73.236.146.240	37215	TCP
2024-12-22T09:54:38.496081+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60908	157.71.90.84	37215	TCP
2024-12-22T09:54:38.496137+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42170	157.78.27.118	37215	TCP
2024-12-22T09:54:38.496227+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52476	41.74.127.201	37215	TCP
2024-12-22T09:54:38.496319+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59638	168.9.251.160	37215	TCP
2024-12-22T09:54:38.496427+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39538	197.204.142.41	37215	TCP
2024-12-22T09:54:38.496495+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38768	157.246.222.210	37215	TCP
2024-12-22T09:54:38.496588+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58432	197.49.210.133	37215	TCP
2024-12-22T09:54:38.496748+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56604	157.99.0.5	37215	TCP
2024-12-22T09:54:38.496850+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34850	157.114.239.129	37215	TCP
2024-12-22T09:54:38.496879+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48056	41.252.95.64	37215	TCP
2024-12-22T09:54:38.496919+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34202	197.143.191.215	37215	TCP
2024-12-22T09:54:38.496979+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50740	197.53.200.178	37215	TCP
2024-12-22T09:54:38.497075+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54776	41.4.212.117	37215	TCP
2024-12-22T09:54:38.497171+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56550	204.60.41.96	37215	TCP
2024-12-22T09:54:38.497332+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44100	44.195.26.98	37215	TCP
2024-12-22T09:54:38.497502+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37608	200.144.159.121	37215	TCP
2024-12-22T09:54:38.497526+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55670	41.13.211.217	37215	TCP
2024-12-22T09:54:38.515625+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37368	59.150.13.216	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:38.515968+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37132	41.38.58.97	37215	TCP
2024-12-22T09:54:38.515988+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47290	169.214.116.84	37215	TCP
2024-12-22T09:54:38.516022+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34306	41.253.208.36	37215	TCP
2024-12-22T09:54:38.516428+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58068	125.116.98.8	37215	TCP
2024-12-22T09:54:38.516537+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42002	72.242.27.0	37215	TCP
2024-12-22T09:54:38.516688+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52388	41.81.204.117	37215	TCP
2024-12-22T09:54:38.516848+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32886	157.140.54.232	37215	TCP
2024-12-22T09:54:38.517111+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50986	145.231.85.209	37215	TCP
2024-12-22T09:54:38.517257+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35894	149.150.35.157	37215	TCP
2024-12-22T09:54:38.517373+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48102	157.218.145.184	37215	TCP
2024-12-22T09:54:38.517468+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41426	166.22.215.243	37215	TCP
2024-12-22T09:54:38.517619+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58076	197.142.192.249	37215	TCP
2024-12-22T09:54:38.517824+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47098	41.55.41.127	37215	TCP
2024-12-22T09:54:38.518010+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38174	157.112.144.13	37215	TCP
2024-12-22T09:54:38.518255+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50126	118.74.60.100	37215	TCP
2024-12-22T09:54:38.518362+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51462	157.16.108.38	37215	TCP
2024-12-22T09:54:38.518655+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49354	157.100.25.0	37215	TCP
2024-12-22T09:54:38.518855+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36596	41.217.226.146	37215	TCP
2024-12-22T09:54:38.518996+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44932	41.135.6.82	37215	TCP
2024-12-22T09:54:38.546751+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42244	41.25.226.250	37215	TCP
2024-12-22T09:54:38.869555+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40528	41.190.102.15	37215	TCP
2024-12-22T09:54:40.607511+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59610	124.56.12.207	37215	TCP
2024-12-22T09:54:40.781468+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41512	182.67.182.239	37215	TCP
2024-12-22T09:54:40.781479+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37352	197.206.178.124	37215	TCP
2024-12-22T09:54:40.781548+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35194	197.94.246.245	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:40.781792+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55514	197.133.226.219	37215	TCP
2024-12-22T09:54:40.781963+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33742	41.38.152.172	37215	TCP
2024-12-22T09:54:40.782200+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57400	197.123.182.53	37215	TCP
2024-12-22T09:54:40.782348+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52822	41.116.195.79	37215	TCP
2024-12-22T09:54:40.782483+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44960	41.88.192.239	37215	TCP
2024-12-22T09:54:40.782611+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58944	197.117.106.197	37215	TCP
2024-12-22T09:54:40.783091+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35398	42.216.162.168	37215	TCP
2024-12-22T09:54:40.783131+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36800	157.46.40.255	37215	TCP
2024-12-22T09:54:40.783260+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53260	157.250.128.244	37215	TCP
2024-12-22T09:54:40.783409+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40598	157.137.156.165	37215	TCP
2024-12-22T09:54:40.783581+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53628	157.61.65.41	37215	TCP
2024-12-22T09:54:40.783662+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57454	197.250.38.147	37215	TCP
2024-12-22T09:54:40.783869+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55486	41.210.110.36	37215	TCP
2024-12-22T09:54:40.783902+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57470	157.238.227.136	37215	TCP
2024-12-22T09:54:40.783949+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44884	77.78.75.11	37215	TCP
2024-12-22T09:54:40.784179+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56400	157.164.243.5	37215	TCP
2024-12-22T09:54:40.784443+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56608	83.251.205.79	37215	TCP
2024-12-22T09:54:40.784607+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45808	157.193.221.66	37215	TCP
2024-12-22T09:54:40.812520+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56542	157.26.190.153	37215	TCP
2024-12-22T09:54:40.812650+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44902	44.217.2.246	37215	TCP
2024-12-22T09:54:40.812738+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60744	46.237.90.246	37215	TCP
2024-12-22T09:54:40.812826+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46716	87.189.117.106	37215	TCP
2024-12-22T09:54:40.812944+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44232	157.184.104.236	37215	TCP
2024-12-22T09:54:40.813048+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60654	41.96.22.70	37215	TCP
2024-12-22T09:54:40.813154+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37556	157.24.162.212	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:40.813313+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57546	41.248.52.181	37215	TCP
2024-12-22T09:54:40.813447+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58998	186.74.79.219	37215	TCP
2024-12-22T09:54:40.813691+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49818	167.206.120.16	37215	TCP
2024-12-22T09:54:40.890916+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34890	157.104.26.138	37215	TCP
2024-12-22T09:54:40.906322+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37134	41.242.37.115	37215	TCP
2024-12-22T09:54:40.906499+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50736	41.24.255.232	37215	TCP
2024-12-22T09:54:40.906650+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48592	41.25.2.169	37215	TCP
2024-12-22T09:54:40.906850+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38296	79.173.82.161	37215	TCP
2024-12-22T09:54:40.906866+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57404	41.144.232.17	37215	TCP
2024-12-22T09:54:40.906992+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45156	131.54.22.125	37215	TCP
2024-12-22T09:54:40.907135+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54942	157.243.44.244	37215	TCP
2024-12-22T09:54:40.939261+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34768	197.58.173.204	37215	TCP
2024-12-22T09:54:41.017638+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48474	41.250.49.135	37215	TCP
2024-12-22T09:54:41.047371+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46540	164.115.182.70	37215	TCP
2024-12-22T09:54:41.062584+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36710	207.115.153.182	37215	TCP
2024-12-22T09:54:41.062951+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54574	103.121.219.225	37215	TCP
2024-12-22T09:54:41.156331+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45192	157.144.162.5	37215	TCP
2024-12-22T09:54:41.156479+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36484	171.174.72.57	37215	TCP
2024-12-22T09:54:41.187794+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45574	41.5.29.7	37215	TCP
2024-12-22T09:54:41.265732+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32820	157.82.121.176	37215	TCP
2024-12-22T09:54:41.281483+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40362	157.1.117.90	37215	TCP
2024-12-22T09:54:41.296951+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38338	197.138.125.200	37215	TCP
2024-12-22T09:54:41.406247+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52528	157.83.176.10	37215	TCP
2024-12-22T09:54:41.430609+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55068	157.123.58.5	37215	TCP
2024-12-22T09:54:41.437804+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34206	157.157.167.235	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:41.688113+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47842	157.16.14.96	37215	TCP
2024-12-22T09:54:41.688147+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38702	157.49.70.213	37215	TCP
2024-12-22T09:54:41.703529+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54134	157.176.36.22	37215	TCP
2024-12-22T09:54:41.703566+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60544	41.13.80.121	37215	TCP
2024-12-22T09:54:41.703654+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56512	197.58.7.230	37215	TCP
2024-12-22T09:54:41.703740+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54470	41.96.151.187	37215	TCP
2024-12-22T09:54:41.703857+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57404	41.242.122.130	37215	TCP
2024-12-22T09:54:41.703887+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57348	197.225.131.194	37215	TCP
2024-12-22T09:54:41.718755+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41318	197.95.9.30	37215	TCP
2024-12-22T09:54:41.718825+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51922	157.143.167.162	37215	TCP
2024-12-22T09:54:41.718918+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38464	197.145.155.50	37215	TCP
2024-12-22T09:54:41.718981+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56102	157.4.23.62	37215	TCP
2024-12-22T09:54:41.719149+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46278	157.77.41.74	37215	TCP
2024-12-22T09:54:41.719215+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35748	157.179.118.157	37215	TCP
2024-12-22T09:54:41.719459+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44704	41.5.6.92	37215	TCP
2024-12-22T09:54:41.719631+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45382	157.176.221.235	37215	TCP
2024-12-22T09:54:41.734663+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52608	197.53.204.94	37215	TCP
2024-12-22T09:54:41.734795+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58526	41.105.3.172	37215	TCP
2024-12-22T09:54:41.734934+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59816	157.136.206.53	37215	TCP
2024-12-22T09:54:41.735065+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35674	197.105.29.188	37215	TCP
2024-12-22T09:54:41.735196+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55748	70.224.88.35	37215	TCP
2024-12-22T09:54:41.735250+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41398	41.134.42.230	37215	TCP
2024-12-22T09:54:41.735464+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34864	41.70.93.7	37215	TCP
2024-12-22T09:54:41.735623+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52808	157.196.42.251	37215	TCP
2024-12-22T09:54:41.735663+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47282	95.48.20.248	37215	TCP

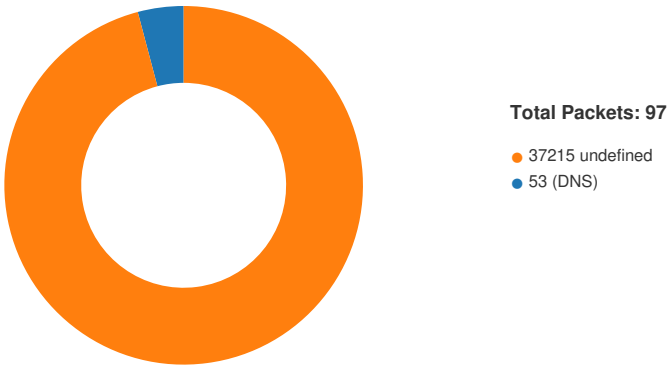
Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:41.735761+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47936	13.114.93.184	37215	TCP
2024-12-22T09:54:41.736111+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60720	41.100.60.118	37215	TCP
2024-12-22T09:54:41.736493+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45652	193.169.72.207	37215	TCP
2024-12-22T09:54:41.736550+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55458	197.230.15.134	37215	TCP
2024-12-22T09:54:41.736783+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43994	41.1.2.236	37215	TCP
2024-12-22T09:54:41.736928+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41746	197.152.93.63	37215	TCP
2024-12-22T09:54:41.737027+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51782	198.121.91.100	37215	TCP
2024-12-22T09:54:41.737124+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55382	41.217.152.254	37215	TCP
2024-12-22T09:54:41.737316+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52428	197.100.171.57	37215	TCP
2024-12-22T09:54:41.737406+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46058	41.114.75.249	37215	TCP
2024-12-22T09:54:41.737512+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37718	197.109.236.163	37215	TCP
2024-12-22T09:54:41.737618+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57170	41.5.171.252	37215	TCP
2024-12-22T09:54:41.766043+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49922	197.26.20.125	37215	TCP
2024-12-22T09:54:41.766048+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49472	197.238.157.241	37215	TCP
2024-12-22T09:54:41.781506+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55758	157.201.162.7	37215	TCP
2024-12-22T09:54:41.812526+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34936	157.145.67.77	37215	TCP
2024-12-22T09:54:41.843719+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	33350	197.195.24.196	37215	TCP
2024-12-22T09:54:41.859363+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38262	157.11.182.118	37215	TCP
2024-12-22T09:54:41.875164+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41376	41.80.131.73	37215	TCP
2024-12-22T09:54:41.875337+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51542	197.92.139.2	37215	TCP
2024-12-22T09:54:41.937719+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57866	157.167.79.27	37215	TCP
2024-12-22T09:54:41.937751+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41548	157.81.173.157	37215	TCP
2024-12-22T09:54:41.937818+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55190	73.34.249.158	37215	TCP
2024-12-22T09:54:41.937988+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48176	157.182.188.210	37215	TCP
2024-12-22T09:54:41.938111+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	58648	157.75.155.137	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:41.938181+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42120	41.36.126.225	37215	TCP
2024-12-22T09:54:41.953203+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50676	175.177.109.173	37215	TCP
2024-12-22T09:54:42.031842+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45432	197.61.64.28	37215	TCP
2024-12-22T09:54:42.063089+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35150	197.221.215.197	37215	TCP
2024-12-22T09:54:42.187758+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50512	197.192.96.16	37215	TCP
2024-12-22T09:54:42.203525+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43530	219.29.99.205	37215	TCP
2024-12-22T09:54:42.302974+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	54212	157.254.38.151	37215	TCP
2024-12-22T09:54:43.750420+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53640	197.75.16.74	37215	TCP
2024-12-22T09:54:43.750638+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56028	157.59.212.110	37215	TCP
2024-12-22T09:54:43.750704+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35388	41.55.213.127	37215	TCP
2024-12-22T09:54:43.750844+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36592	42.45.214.215	37215	TCP
2024-12-22T09:54:43.765924+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57612	157.47.76.164	37215	TCP
2024-12-22T09:54:43.766059+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	36736	76.150.202.9	37215	TCP
2024-12-22T09:54:43.766312+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50898	157.203.117.14	37215	TCP
2024-12-22T09:54:43.766453+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42798	197.215.106.211	37215	TCP
2024-12-22T09:54:43.766756+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49420	197.179.216.8	37215	TCP
2024-12-22T09:54:43.777402+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39296	180.70.144.212	37215	TCP
2024-12-22T09:54:43.781527+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50012	197.32.203.12	37215	TCP
2024-12-22T09:54:43.781605+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55172	197.41.98.107	37215	TCP
2024-12-22T09:54:43.781789+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51426	159.187.203.35	37215	TCP
2024-12-22T09:54:43.782006+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39526	157.30.72.180	37215	TCP
2024-12-22T09:54:43.782007+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41602	41.151.165.203	37215	TCP
2024-12-22T09:54:43.782055+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56316	41.52.171.173	37215	TCP
2024-12-22T09:54:43.782313+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51054	197.22.19.95	37215	TCP
2024-12-22T09:54:43.782499+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37634	65.120.78.60	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:43.782592+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57082	197.22.128.155	37215	TCP
2024-12-22T09:54:43.797123+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39394	41.78.254.164	37215	TCP
2024-12-22T09:54:43.797149+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	48274	157.220.79.206	37215	TCP
2024-12-22T09:54:43.797194+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	56918	176.139.201.142	37215	TCP
2024-12-22T09:54:43.797261+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	41750	157.212.81.222	37215	TCP
2024-12-22T09:54:43.797289+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	42710	157.156.34.139	37215	TCP
2024-12-22T09:54:43.812925+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45994	197.226.154.83	37215	TCP
2024-12-22T09:54:43.812991+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59616	197.253.237.105	37215	TCP
2024-12-22T09:54:43.813139+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57636	197.128.28.245	37215	TCP
2024-12-22T09:54:43.813178+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53912	197.231.67.45	37215	TCP
2024-12-22T09:54:43.813241+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43640	157.147.195.237	37215	TCP
2024-12-22T09:54:43.813801+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44282	74.235.31.132	37215	TCP
2024-12-22T09:54:43.860401+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52054	197.126.80.72	37215	TCP
2024-12-22T09:54:43.860510+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45928	46.180.127.93	37215	TCP
2024-12-22T09:54:43.860559+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59736	198.239.207.90	37215	TCP
2024-12-22T09:54:43.891014+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	47356	53.216.118.225	37215	TCP
2024-12-22T09:54:43.891083+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35948	44.221.220.67	37215	TCP
2024-12-22T09:54:43.922345+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35908	197.164.231.239	37215	TCP
2024-12-22T09:54:44.062724+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57328	157.11.143.98	37215	TCP
2024-12-22T09:54:44.890852+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	49790	41.88.200.41	37215	TCP
2024-12-22T09:54:44.890914+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	35208	197.9.237.197	37215	TCP
2024-12-22T09:54:44.906838+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	37416	197.94.61.31	37215	TCP
2024-12-22T09:54:44.906922+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	34874	41.204.249.60	37215	TCP
2024-12-22T09:54:44.907395+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53502	41.205.209.113	37215	TCP
2024-12-22T09:54:44.907663+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	53836	40.175.206.61	37215	TCP

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-22T09:54:44.907977+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	50062	41.211.176.78	37215	TCP
2024-12-22T09:54:44.908430+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	52772	130.228.151.57	37215	TCP
2024-12-22T09:54:44.908490+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40408	197.249.59.36	37215	TCP
2024-12-22T09:54:44.908774+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55912	197.76.228.50	37215	TCP
2024-12-22T09:54:44.908805+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55908	150.62.199.50	37215	TCP
2024-12-22T09:54:44.908900+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	45724	197.254.64.229	37215	TCP
2024-12-22T09:54:44.909306+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	32824	111.114.109.125	37215	TCP
2024-12-22T09:54:44.909478+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	57226	157.34.203.44	37215	TCP
2024-12-22T09:54:44.909614+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	51640	197.214.225.35	37215	TCP
2024-12-22T09:54:44.937783+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60742	197.157.158.72	37215	TCP
2024-12-22T09:54:44.937895+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	60476	41.4.228.252	37215	TCP
2024-12-22T09:54:44.938005+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	59752	201.208.96.148	37215	TCP
2024-12-22T09:54:44.939353+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	46184	157.128.230.29	37215	TCP
2024-12-22T09:54:44.939950+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40004	161.23.185.25	37215	TCP
2024-12-22T09:54:44.940376+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	44640	197.30.181.2	37215	TCP
2024-12-22T09:54:44.940868+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	40262	157.162.189.166	37215	TCP
2024-12-22T09:54:44.941366+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38752	197.39.128.160	37215	TCP
2024-12-22T09:54:44.953178+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	55016	197.131.75.140	37215	TCP

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: 3.elf PID: 5558, Parent PID: 5475

General

Start time (UTC):	08:53:40
Start date (UTC):	22/12/2024
Path:	/tmp/3.elf
Arguments:	/tmp/3.elf
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: 3.elf PID: 5566, Parent PID: 5558

General

Start time (UTC):	08:53:43
Start date (UTC):	22/12/2024
Path:	/tmp/3.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 3.elf PID: 5568, Parent PID: 5566

General

Start time (UTC):	08:53:43
Start date (UTC):	22/12/2024
Path:	/tmp/3.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 3.elf PID: 5572, Parent PID: 5568

General

Start time (UTC):	08:53:43
Start date (UTC):	22/12/2024
Path:	/tmp/3.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: 3.elf PID: 5573, Parent PID: 5568

General

Start time (UTC):	08:53:44

Start date (UTC):	22/12/2024
Path:	/tmp/3.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 3.elf PID: **5576**, Parent PID: **5568**

General

Start time (UTC):	08:53:44
Start date (UTC):	22/12/2024
Path:	/tmp/3.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

Directory Enumerated

Analysis Process: xfce4-panel PID: **5560**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/bin/xfce4-panel
Arguments:	-
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5560**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 6 12582920 systray "Notification Area" "Area where notification icons appear"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Analysis Process: xfce4-panel PID: **5561**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/bin/xfce4-panel
Arguments:	-
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5561**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0

Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libstatusnotifier.so 7 12582921 statusnotifier "Status Notifier Plugin" "Provides a panel area for status notifier items (application indicators)"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Analysis Process: xfce4-panel PID: **5562**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/bin/xfce4-panel
Arguments:	-
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5562**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 8 12582922 pulseaudio "PulseAudio Plugin" "Adjust the audio volume of the PulseAudio sound system"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Analysis Process: xfce4-panel PID: **5563**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/bin/xfce4-panel
Arguments:	-
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5563**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 9 12582923 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Analysis Process: xfce4-panel PID: **5564**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/bin/xfce4-panel
Arguments:	-
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5564**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Analysis Process: xfce4-panel PID: **5565**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/bin/xfce4-panel
Arguments:	-
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5565**, Parent PID: **3172**

General

Start time (UTC):	08:53:41
Start date (UTC):	22/12/2024
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 14 12582925 actions "Action Buttons" "Log out, lock or other system actions"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read