Hunting for Cobalt Strike in PCAP

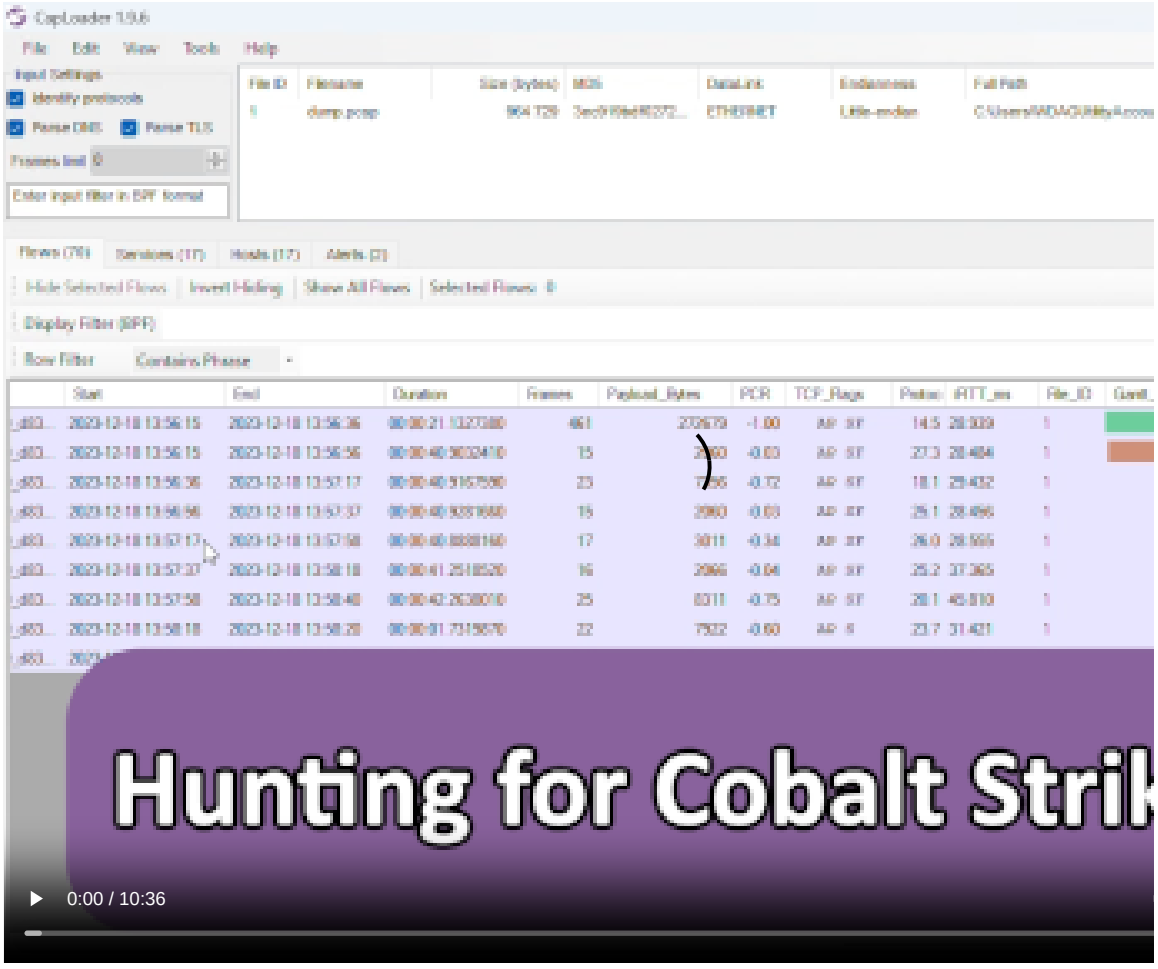
By Erik Hjelmvik

Published: 2024-01-04 · Archived: 2026-04-05 17:39:42 UTC

,

Thursday, 04 January 2024 10:12:00 (UTC/GMT)

In this video I analyze a pcap file with network traffic from Cobalt Strike Beacon using CapLoader.



The pcap file and Cobalt Strike malware config can be downloaded from Recorded Future's Triage sandbox.

Cobalt Strike Beacon configs can also be extracted locally with help of Didier Stevens' 1768.py or Fox-IT's dissect.cobaltstrike.

IOC List

- MD5 99516071d8f3e78e51200948bf377c4c
- SHA1 59fe505b24bdfa54ee6e4188ed8b88af9a42eb86
- SHA256 10e68f3e6c73161a1bba85ef9bada0cd79e25382ea8f8635bec4aa51bfe6c707
- JA3 a0e9f5d64349fb13191bc781f81f42e1
- JA4 t12d190800_d83cc789557e_7af1ed941c26
- IP:port 104.21.88.185:2096 (Cloudflare)
- Domain mail.googlesmail.xyz (Go Daddy)

Network Forensics Training

Are you interested in learning more about how to analyze network traffic from Cobalt Strike and other backdoors, malware and hacker tools? Then take a look at our upcoming network forensics classes!

Posted by Erik Hjelmvik on Thursday, 04 January 2024 10:12:00 (UTC/GMT)

Tags: #Cobalt Strike#CobaltStrike#Triage#JA3#a0e9f5d64349fb13191bc781f81f42e1#ThreatFox#CapLoader#Video #videotutorial

Short URL: https://netresec.com/?b=2410f02
