Detecting PureLogs traffic with CapLoader

By Erik Hjelmvik

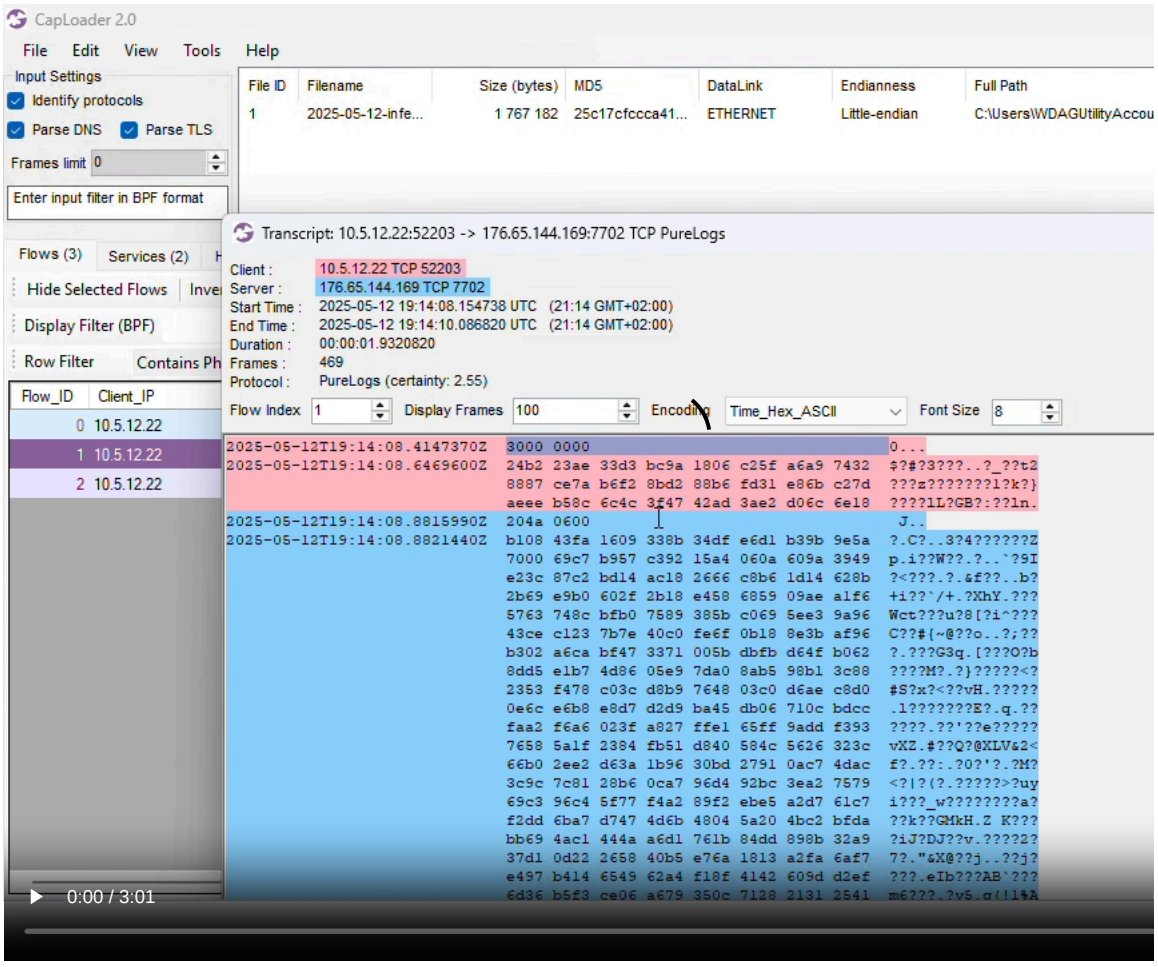
Published: 2025-06-09 · Archived: 2026-04-06 00:04:00 UTC

,

Monday, 09 June 2025 14:26:00 (UTC/GMT)

CapLoader includes a feature for Port Independent Protocol Identification (PIPI), which can detect which protocol is being used inside of TCP and UDP sessions without relying on the port number. In this video CapLoader identifies the C2 protocol used by the PureLogs Stealer malware.

The PureLogs protocol detection was added to CapLoader in the recent 2.0 release.



The PCAP file analyzed in the video is from Brad Duncan's fantastic malware-traffic-analysis.net website.

Indicators of Compromize (IOC):

- mxcnss.dns04.com:7702
- 176.65.144.169:7702

Posted by Erik Hjelmvik on Monday, 09 June 2025 14:26:00 (UTC/GMT)

Tags: #CapLoader#PureLogs#malware-traffic-analysis.net#PIPI

Short URL: https://netresec.com/?b=256a8c4