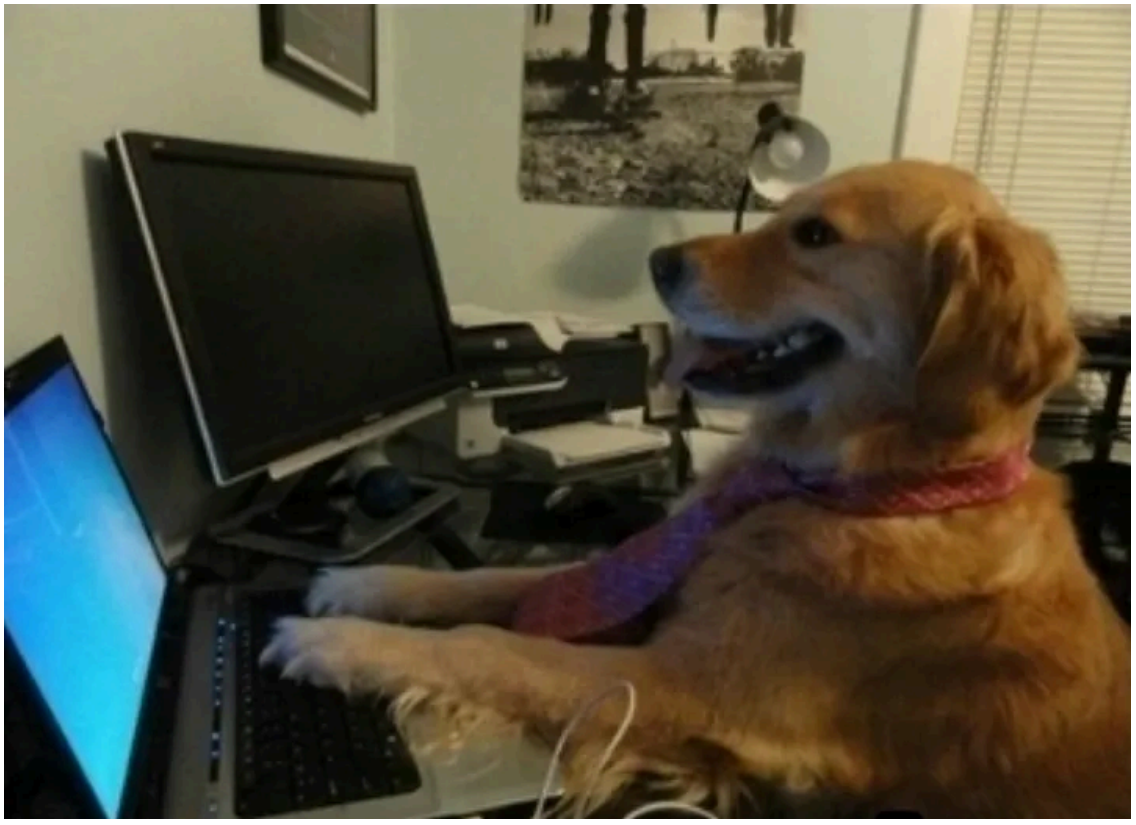
Cobalt Strike Hunting — DLL Hijacking/Attack Analysis

By Michael Koczwara

Published: 2022-06-13 · Archived: 2026-04-05 18:52:43 UTC

DLL Hijacking via Cobalt Strike & Attack Analysis.

Press enter or click to view image in full size



Agenda

- Hijack Execution Flow: DLL Search Order Hijacking.
- Payload extraction from the PCAP (VT, Triage, and CyberChef Analysis).
- Attack Analysis.
- DLL Hijacking via Cobalt Strike/Sysrep.

Hijack Execution Flow

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over

time. Adversaries may also use these mechanisms to elevate privileges or evade defences, such as application control or other restrictions on execution.

There are many ways an adversary may hijack the flow of execution, including by:

- Manipulating how the operating system locates programs to be executed.
- How the operating system locates libraries to be used by a program can also be intercepted.
- Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.
