Cobalt Strike Hunting — DLL Hijacking/Attack Analysis

michaelkoczwara.medium.com/cobalt-strike-hunting-dll-hijacking-attack-analysis-ffbf8fd66a4e

Michael Koczwara December 30, 2021

Michael Koczwara

Aug 17, 2021

.

6 min read

DLL Hijacking via Cobalt Strike & Attack Analysis.

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.

--

Recommended from Medium

Novan

Conflicker and its legacy: An Overview of the Conficker worm.

Kamran Saifullah

Practical Malware Analysis—Chapter 1—Lab 01–04—Solution