New Tool: cs-extract-key.py

Published: 2021-11-03 · Archived: 2026-04-05 20:16:25 UTC

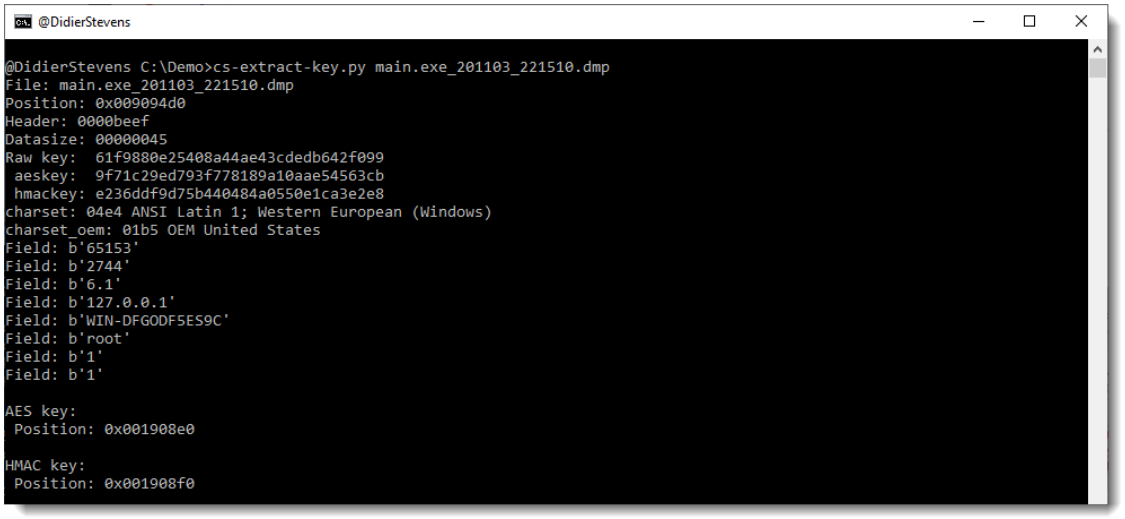
New Tool: cs-extract-key.py

cs-extract-key.py is a tool designed to extract cryptographic keys from Cobalt Strike beacon process memory dumps.

This tool was already available in my beta repository.

This tool can extract cryptographic keys from process memory dumps of a version 3.x beacon directly:

And from version 4.x together with encrypted data extracted from network capture:



More details can be found in the man page, and in and upcoming blog post.

cs-extract-key_V0_0_1.zip (https)
MD5: 4102A5A5BFD4D432DA4A721D43F568F5
SHA256: BBEDF6CBFFF51669187694F463C32A49F53420BEDF8B76508D06850643DE334F
