

Cobalt Strike: Overview – Part 7

By Didier Stevens

Published: 2022-03-22 · Archived: 2026-04-05 21:35:13 UTC

This is an overview of a series of 6 blog posts we dedicated to the analysis and decryption of Cobalt Strike traffic. We include videos for different analysis methods.

In [part 1](#), we explain that Cobalt Strike traffic is encrypted using RSA and AES cryptography, and that we found private RSA keys that can help with decryption of Cobalt Strike traffic

In [part 2](#), we actually decrypt traffic using private keys. Notice that one of the free, open source tools that we created to decrypt Cobalt Strike traffic, [cs-parse-http-traffic.py](#), was a beta release. It has now been replaced by tool [cs-parse-traffic.py](#). This tool is capable to decrypt HTTP(S) and DNS traffic. For HTTP(S), it's a drop-in replacement for cs-parse-http-traffic.py.

In [part 3](#), we use process memory dumps to extract the decryption keys. This is for use cases where we don't have the private keys.

In [part 4](#), we deal with some specific obfuscation: data transforms of encrypted traffic, and sleep mode in beacons' process memory.

In [part 5](#), we handle Cobalt Strike DNS traffic.

And finally, in [part 6](#), we provide some tips to make memory dumps of Cobalt Strike beacons.

The tools used in these blog post are free and open source, and can be found [here](#).

Here are a couple of videos that illustrate the methods discussed in this series:

- [Using Known Private Keys To Decrypt Traffic](#)
- [Using Process Memory To Decrypt Traffic](#)
- [Dealing With Obfuscated Traffic And Process Memory](#)
- [Decrypting DNS Traffic](#)

YouTube playlist "[Cobalt Strike: Decrypting Traffic](#)"

Blog posts in this series:

- [Cobalt Strike: Using Known Private Keys To Decrypt Traffic – Part 1](#)
- [Cobalt Strike: Using Known Private Keys To Decrypt Traffic – Part 2](#)
- [Cobalt Strike: Using Process Memory To Decrypt Traffic – Part 3](#)
- [Cobalt Strike: Decrypting Obfuscated Traffic – Part 4](#)
- [Cobalt Strike: Decrypting DNS Traffic – Part 5](#)

- [Cobalt Strike: Memory Dumps – Part 6](#)

About the authors

Didier Stevens is a malware expert working for NVISIO. Didier is a SANS Internet Storm Center senior handler and Microsoft MVP, and has developed numerous popular tools to assist with malware analysis. You can find Didier on [Twitter](#) and [LinkedIn](#).

You can follow NVISIO Labs on [Twitter](#) to stay up to date on all our future research and publications.

Published March 22, 2022March 22, 2022

Post navigation

Source: <https://blog.nviso.eu/2022/03/22/cobalt-strike-overview-part-7/>