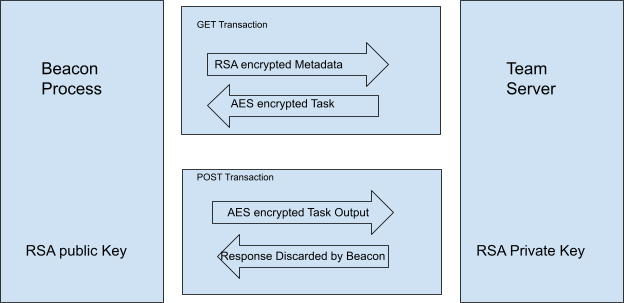
Starter Kit

This document aims to help you solve step 2 of our challenge. Even with this information, solving it will be challenging. Nevertheless, we hope that you will learn something and enjoy it.

Cobalt Strike

Cobalt Strike is a C2 framework that executes a beacon (payload) on a targeted computer. This beacon communicates with the Team Server (C2 server) using a combination of symmetric (AES) and asymmetric (RSA) encryption key algorithms.



The beacon in the metadata sends the AES key. It means that if we know the RSA private key, we can find the AES key and decrypt the Task and the Task Output.

Some leaked versions are available on the Internet and used by attacker groups. The corresponding private/public RSA keys are known.

You can read these articles to know more.

* <https://unit42.paloaltonetworks.com/cobalt-strike-metadata-encryption-decryption/>
* <https://unit42.paloaltonetworks.com/cobalt-strike-metadata-encoding-decoding/>

All the tools you need are available in this repository:

* <https://github.com/DidierStevens/DidierStevensSuite>

Files downloaded by Cobalt Strike

When the operator downloads files from the beacon, they are sent in chunks. For this reason, it might be interesting to rebuild the chunks in the right order to get back the downloaded file.

This oneliner is an example of using Bash to accomplish that.

IFS=$'\n'; for line in `grep -A2 CALLBACK\_FILE\_WRITE cobalt\_strike\_communication.txt | grep MD5` ; do VAR=`echo $line | cut -d ' ' -f3`; cat "payload-$VAR.vir" >> downloaded\_file ; done

Mimikatz

Mimikatz is the tool to use on Windows when you want to extract secrets from a minidump.

Articles to read

* <https://tools.thehacker.recipes/mimikatz/modules/sekurlsa/cloudap>
* <https://tools.thehacker.recipes/mimikatz/modules/dpapi/cloudapkd>
* <https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token>
* <https://dirkjanm.io/introducing-roadtools-token-exchange-roadtx/>