

New Tool: cs-extract-key.py

blog.didierstevens.com/2021/11/03/new-tool-cs-extract-key-py/

November 3, 2021

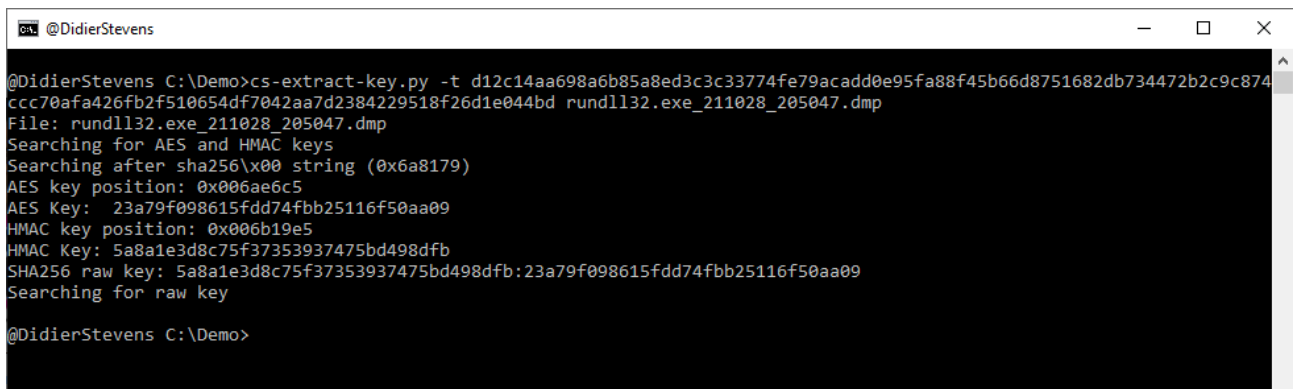
Wednesday 3 November 2021

Filed under: [Announcement](#), [Encryption](#), [My Software](#) — Didier Stevens @ 0:00

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](#).

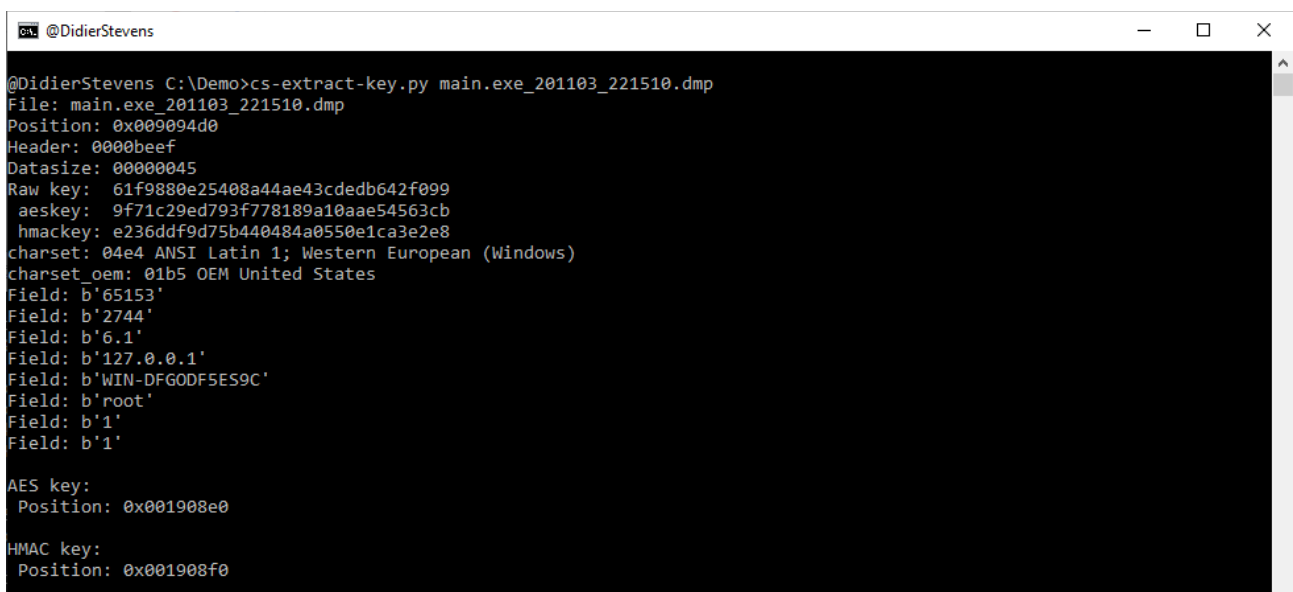
This tool can extract cryptographic keys from process memory dumps of a version 3.x beacon directly:



```
@DidierStevens C:\Demo>cs-extract-key.py -t d12c14aa698a6b85a8ed3c3c33774fe79acadd0e95fa88f45b66d8751682db734472b2c9c874ccc70afa426fb2f510654df7042aa7d2384229518f26d1e044bd rundll32.exe_211028_205047.dmp
File: rundll32.exe_211028_205047.dmp
Searching for AES and HMAC keys
Searching after sha256\x00 string (0x6a8179)
AES key position: 0x006ae6c5
AES Key: 23a79f098615fdd74fbb25116f50aa09
HMAC key position: 0x006b19e5
HMAC Key: 5a8a1e3d8c75f37353937475bd498dfb
SHA256 raw key: 5a8a1e3d8c75f37353937475bd498dfb:23a79f098615fdd74fbb25116f50aa09
Searching for raw key

@DidierStevens C:\Demo>
```

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



```
@DidierStevens C:\Demo>cs-extract-key.py main.exe_201103_221510.dmp
File: main.exe_201103_221510.dmp
Position: 0x009094d0
Header: 0000beef
Datatype: 00000045
Raw key: 61f9880e25408a44ae43cdeb642f099
aeskey: 9f71c29ed793f778189a10aae54563cb
hmackey: e236ddf9d75b440484a0550e1ca3e2e8
charset: 04e4 ANSI Latin 1; Western European (Windows)
charset_oem: 01b5 OEM United States
Field: b'65153'
Field: b'2744'
Field: b'6.1'
Field: b'127.0.0.1'
Field: b'WIN-DFGODF5ES9C'
Field: b'root'
Field: b'1'
Field: b'1'

AES key:
Position: 0x001908e0

HMAC key:
Position: 0x001908f0
```

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

[Comments \(1\)](#)

1 Comment »

1. [...] New Tool: cs-extract-key.py [...]

Pingback by [Week 45 – 2021 – This Week In 4n6](#) — Sunday 7 November 2021 @ 11:10

[RSS \(Really Simple Syndication\)](#) feed for comments on this post. [TrackBack URI \(Uniform Resource Identifier\)](#)

Leave a Reply (comments are moderated)



You are commenting using your WordPress.com account. ([Log Out](#) / [Change](#))



You are commenting using your Twitter account. ([Log Out](#) / [Change](#))



You are commenting using your Facebook account. ([Log Out](#) / [Change](#))

[Cancel](#)

Connecting to %s

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)