**General notes**

* This is a one day class, but can be built out to two days by including ‘student lab time’ and making it more hands on.
* A one day time slot will get you through the slides with minimal demos, and you’ll find yourself rushing somewhat at times.

**Module 1**

Remcos

The labs for this course are based on the free version of the remcos RAT. This is downloadable and lets the participants create simple clients which can later in the class be analysed with the toolset. It also illustrates the more advanced capabilities that are available (although one needs the paid version to create them; at least the ‘tick boxes’ are visible, although ‘grayed out’).

To set up a demo machine, install a Windows OS in a virtual machine, and download the remcos free version from

<https://breaking-security.net/remcos/>

It is also useful to spend some time on this website and talk the participants through the cost structure of some of the options that are available. This is a good illustration of what is available and at what price.

Bonus: look at some of the legal terminology denying all responsibility.

It is also useful to read up on some of the following resources for some background:

<https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.html>

<https://breaking-security.net/>

<http://breaking-security.net/shop/remcos/>

<https://www.youtube.com/watch?v=BVxQxSfNJXQ>

<https://krabsonsecurity.com/2018/03/02/analysing-remcos-rats-executable/>

**MODULE 2: Artefact Analysis**

Lab 2.0: Functionality

It is quite easy to build a small lab on a VM with a remcos controller and a victim. Install the remcos software on the controller and investigate the options, then build a client. Install it on the victim and see what is possible. Make sure the client and victim communicate on a ‘host only’ network.

Note: while interesting, this is in practice a lot more time consuming, during the class, than it seems. Only do this if you have sufficient time. You can also let the students do this themselves.

Remcos builder

Remcos client

Lab 2.1: Packers

Back to the builder.

Use UPX as a packer and build a new client with and without a packer.

Than use some of the packer analysis tooling to investigate the differences.

Lab 2.2: Sandboxing

VT and Hybrid-analysis of the built sample. What do the indicators say?

Lab 2.3: Disassemble the original and packed samples

Disassemble the original and packed samples, e.g. with

Lab 2.4: Volatility

Analyse the victim with volatility

Lab 2.5: Yara

Write a yara signature for your remcos client