Some pointers to useful and interesting lab work alongside the course

MODULE 1: Malware Ecosystem

**Lab 1: Site investigation**

Remcos RAT - free version and some samples

<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>

Remcos Krabs discussion

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

MODULE 2: Artefact Analysis

**Lab 2.0: Functionality**

Remcos builder

Remcos client

**Lab 2.1: Packers**

Back to the builder.

Use UPX as a packer and build a new client

Analyse with a packer solution

**Lab 2.2: Sandboxing**

VT and Hybrid-analysis of just built sample

**Lab 2.3: Disassemble the original and packed samples**

Disassemble the original and packed samples

**Lab 2.4: Volatility**

Analyse the victim with volatility

**Lab 2.5: Yara**

Write a yara signature for your remcos client