Emotet

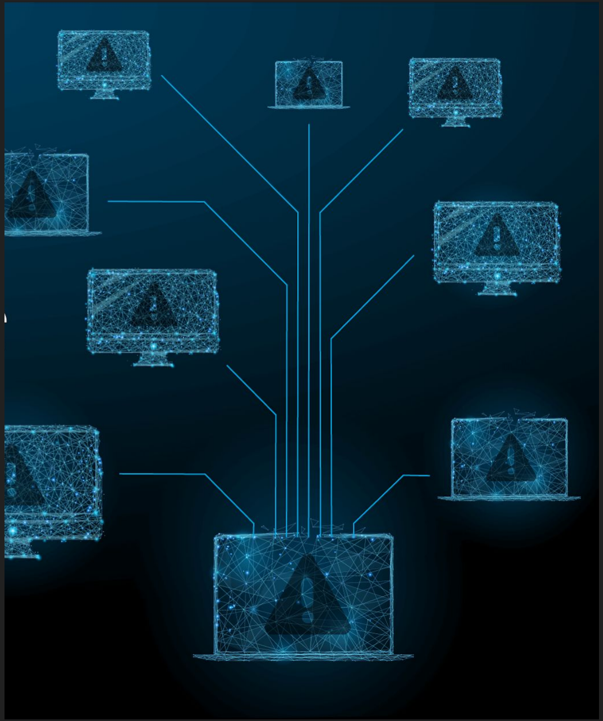
2014 - 2021 (probably)

Emotet

- Developed by highly skilled programmers
- Evolved from targeted banking trojan
  - Modified to spread and communicate across networks

(post ransomware world)

- Began infecting all sorts of organizations and distributing malware (MaaS)
- Really started to profit - devs could literally go on vacation



Emotet Gang (aka Mummy Spider)

- Organized and capable threat actor
  - APT?
- Made up of college grads and skilled software engineers
- Reach-out and recruit skilled criminals
- Pays its EMPLOYEES millions of dollars a year
  - Ya, they literally go on vacation for like half the year

Redundant Botnet and Hunting of Emotet C2s

- Layers of compromised servers form complex botnet web
  - Broken-down into tiers to protect core servers
- Three “Epochs” of Tier 1 C2s
- Considered by many to be invincible

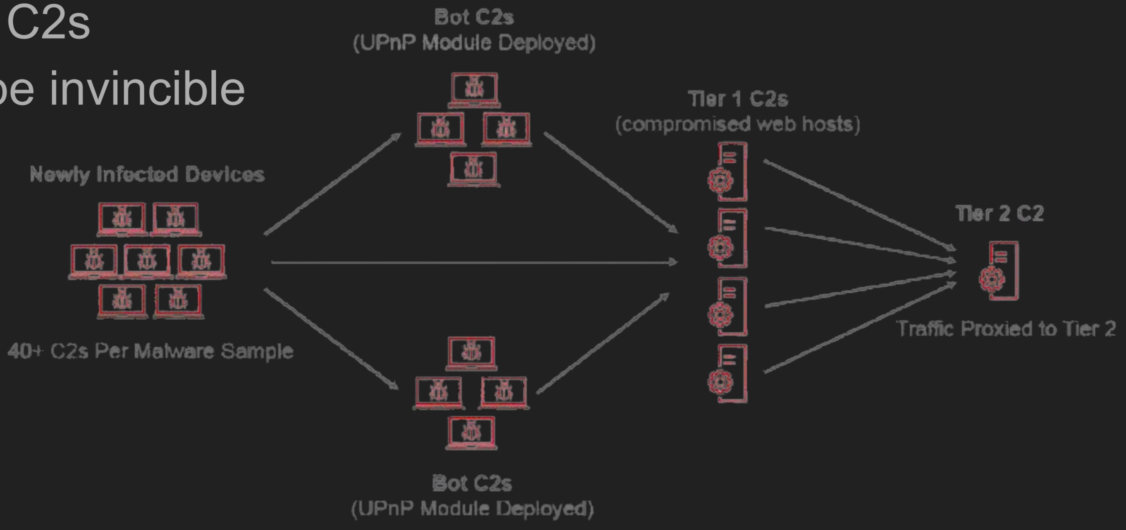
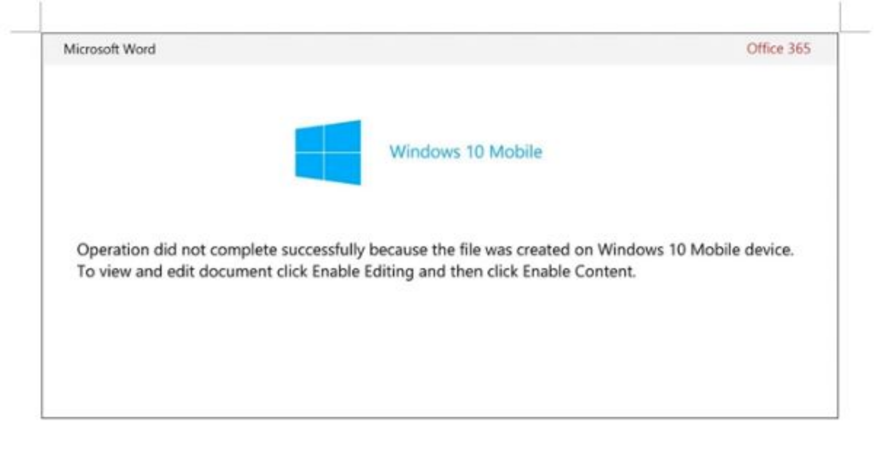


Figure 2: Emotet C2 Architecture

Hunting of Emotet C2s

- Gets tricky with complex botnet, but Emotet pissed-off hackers regardless
- Feodo Tracker
- Cryptolaemus1 forms to “eat some Mealybugs”
    - Track C2 servers
    - Monitor malspam signatures
    - Connect industry experts and defenders



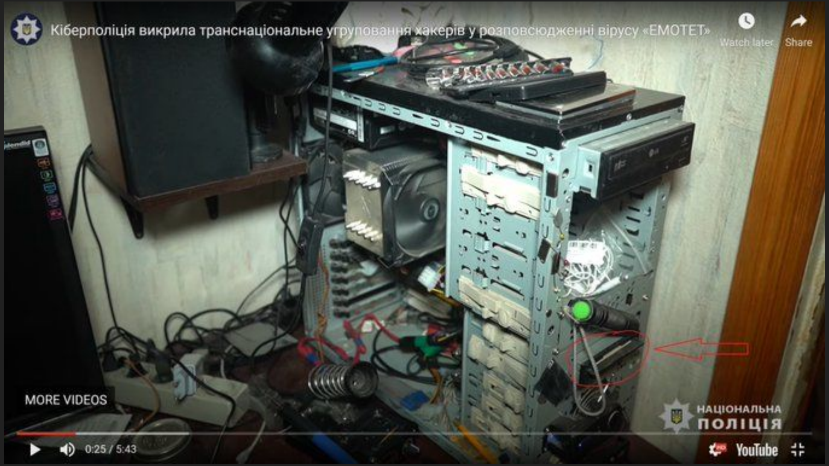
Operation did not complete successfully because the file was created on Windows 10 Mobile device. To view and edit document click Enable Editing and then click Enable Content.

Year of 2020

1. Picked-up during pandemic, but promised to not target healthcare
    - ATTACKED HOSPITALS
2. Developed more relationships with cyber criminals
3. Emotet vaccine discovered by James Quinn
4. US Cyber Command took some swings at botnets
5. Group returns to malspam just after Christmas

The Takedown

- Law enforcement tracked-down the leaders of Emotet gang
- Working with researchers, they rooted-out all the C2s in the botnet
  - Even created automated update to crue still infected
- In coordinated take-down, SWAT teams raided apartment as botnet crumbled
- Local servers taken to help


Кіберполіція викрила транснаціональне угруповання хакерів у розповсюдженні вірусу «EMOTET»

Looking Forward

- Emotet effectively dead, still rooting-out some developers
- Botnet notoriously resistant…
- Possible that malware code could be harvested and reused
- Botnet structure not too sophisticated… similar malware will rise