Online underground markets and hacker forums

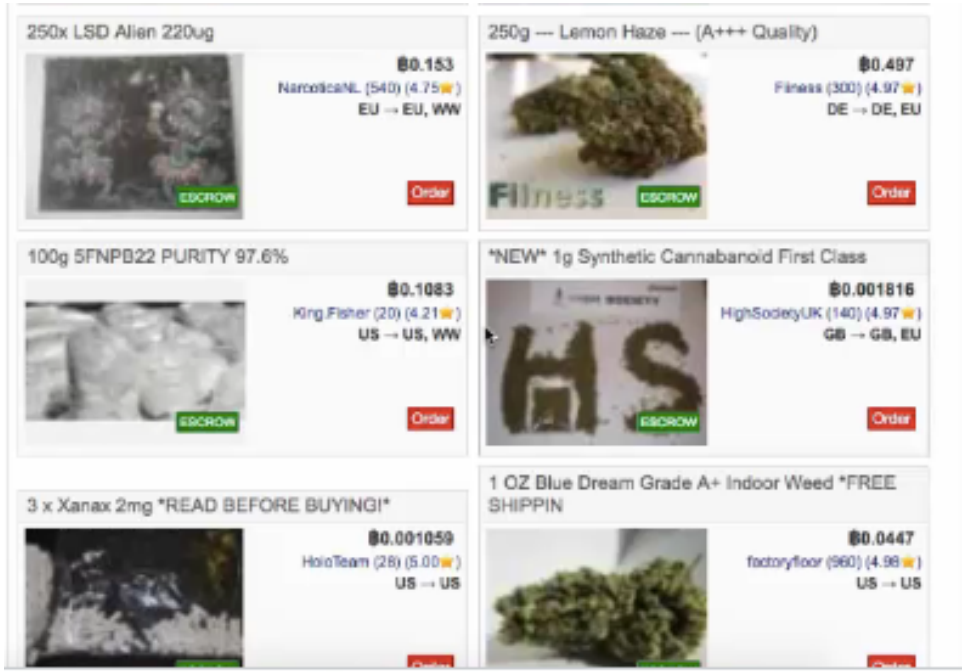
Sergio Pastrana, PhD

Cambridge Cybercrime Centre

Sergio.Pastrana@cl.cam.ac.uk

Underground Marketplaces

- Online markets where both buyers and sellers are anonymous
- Usually serve illegal content



Underground Marketplaces: economics

- **Silk Road**: around $400k a day [Soska & Christin, 2015]
- **AlphaBay**: more than $1 billion between 2015-2017 [www.justice.gov, 2017]

Background on Internet traceability

- IP addresses identify machines on the Internet, and they are traceable
  - Assume www.drugmarket.com -> 12.34.56.78
  - Trace 12.34.56.78, go to address and arrest owner
- Solution (for criminals): The Onion Router (TOR)

TOR hidden services

- Hidden services allows to “offer a web server […] without revealing your IP address to its users” [www.torproject.org]

- Users connect using the TOR browser, by means of "onion addresses”
  - e.g. http://lchudifyeqm4ldjj.onion/

What an online illegal marketplace looks like?

Underground forums

- Online communities where offenders can meet, network and advertise their products
  - Exchange knowledge (tutorials, guides, Q&A, etc.)
  - Discussion topics
  - Marketplace
- Hacker forums
  - Illicit\fraudulent monetizing techniques
  - Hacking material: malware, botnets, exploits, etc.
  - Most of them operate in surface web
    - Not illegal content *per-se*

What an underground forum looks like?