Mason Competitive Cyber

Cybercrime: The Underground Economy

Upcoming Competitions & Events

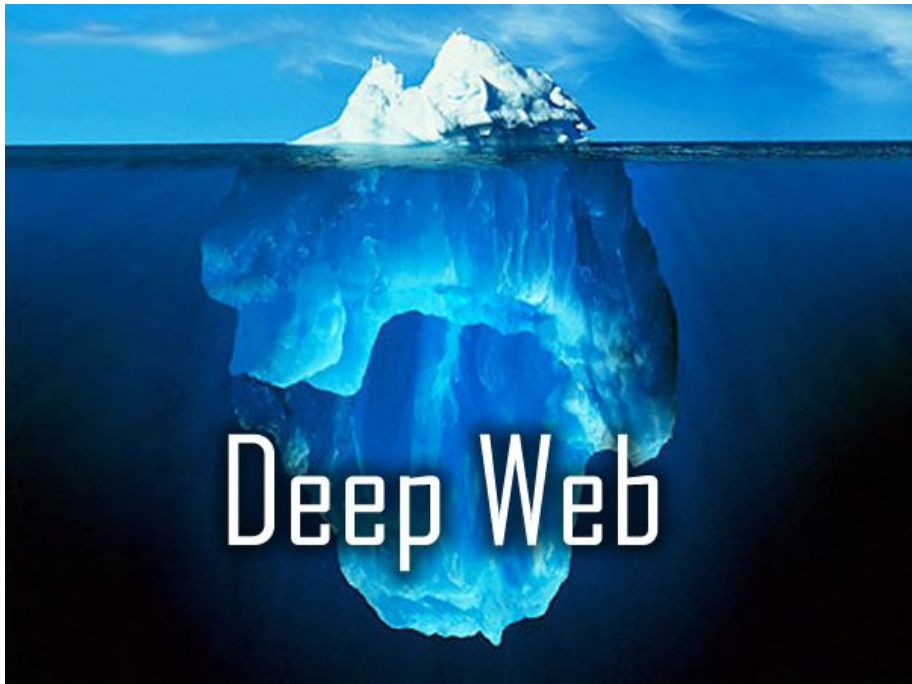
- Last meeting for the semester next week
  - Career Rountable
  - Resume and Job/Internship Searching Advice

Cybercrime

- Disclaimer: don’t do illegal shit
- Darknet
- Crime-as-a-Service (CaaS)
- Traditional crime on the Internet
- Cybercrime

Deep Web vs Darknet

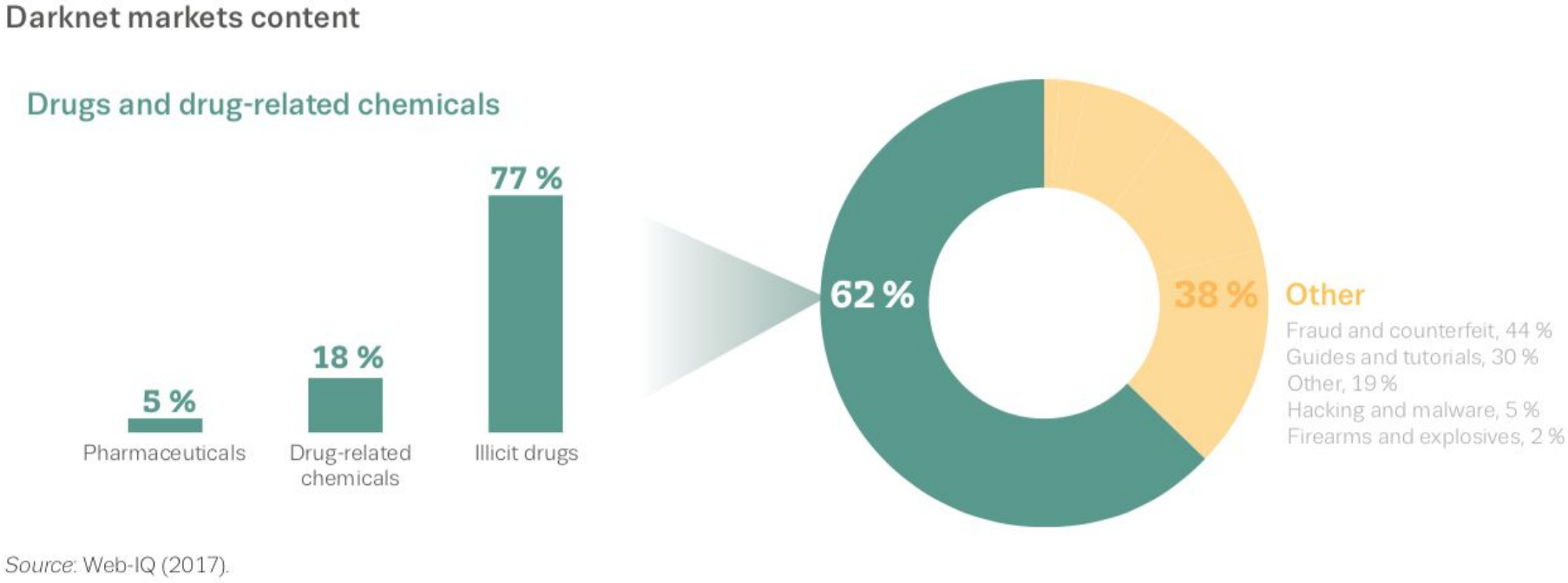
- Deep Web = not indexed by search engines
  - Gmail inbox
  - Cloud storage
- Darknet = parts of Deep Web that can only be accessed with specific software/configurations
  - DN Markets
  - Ransomware websites
  - Hacking forums



Tor

- Anonymity network
- Originally designed by US Navy
- Assigns an anonymous IP address to user
  - Traffic sent through multiple nodes
- Allows access to Darknet
- TAILS
  - Anonymous OS, live USB

For Sale on the Darknet



Source: Web-IQ (2017).

Products

- Drugs
- PII
  - SSNs
  - Credit card numbers, financial data
- Credentials
- Customizable Malware
  - Ransomware
  - Banking malware (Zeus)
- Exploits
- Control of Compromised Machines
- Training - How to be a cyber criminal 101
- Weapons
  - High percentage scammers

Services

- Hitmen
  - 99.9% scammers or undercover cops
- DDoS
- Exploit Kit
  - Monthly
- Infrastructure rental
- Money laundering
  - Cryptocurrencies
    - Tumblers
  - High percentage scammers

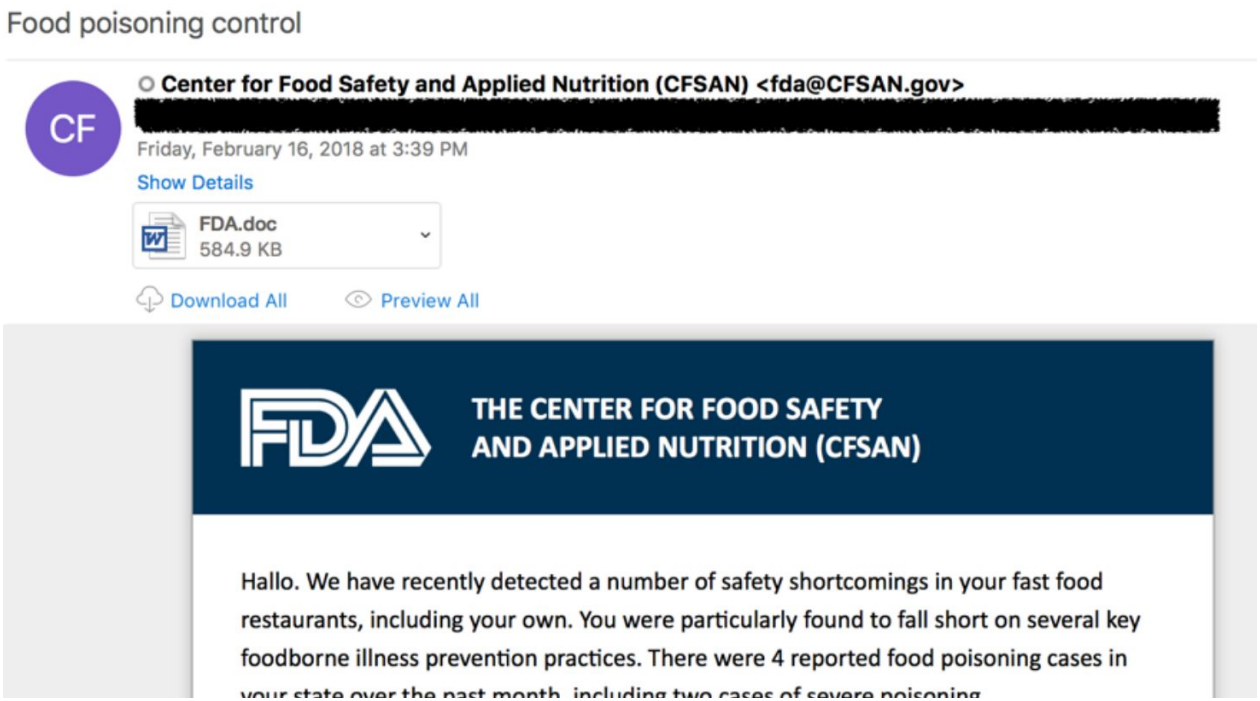
Clickfraud

- Pay-per-click (PPC) advertising
- Affiliate clickfraud
  - Ad placed on site
  - Pay for ad clicks
- Competitive clickfraud
  - Competitor pays for clicks from search engine
  - Click the link to cost them money

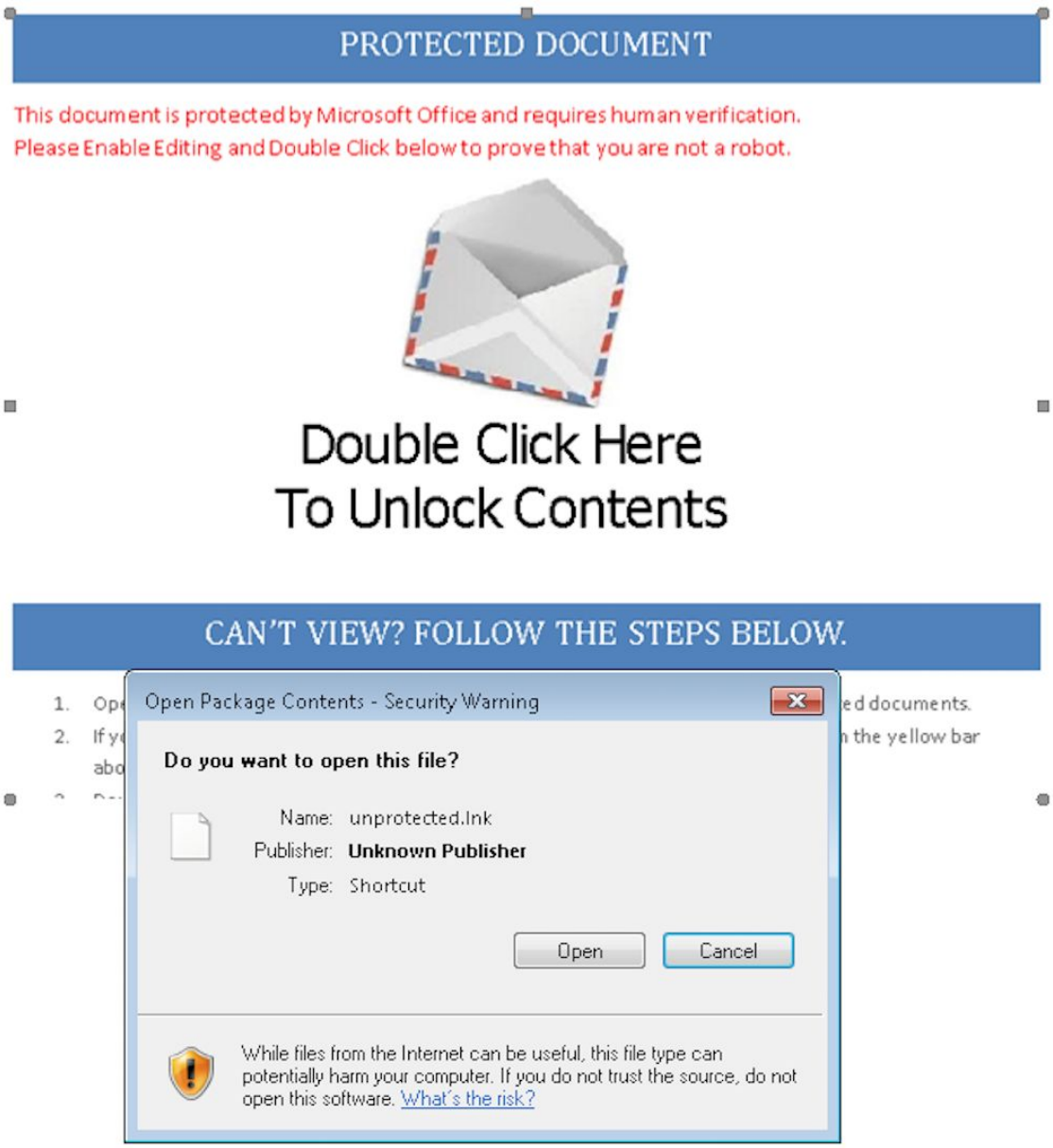
FIN7

- AKA the “Carbanak Group”
- Usually hack large companies to steal CC data
  - Sell on darknet

1) Spear phishing + malicious macros
2) Spear phishing + hidden lnk file + VBscript



FIN7


PROTECTED DOCUMENT
This document is protected by Microsoft Office and requires human verification.
Please Enable Editing and Double Click below to prove that you are not a robot.
Double Click Here
To Unlock Contents
CAN'T VIEW? FOLLOW THE STEPS BELOW.
Open Package Contents - Security Warning
Do you want to open this file?
Name: unprotected.lnk
Publisher: Unknown Publisher
Type: Shortcut
Open
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

How 2 get rich quick buy my ebook for $49.99 I swear it works

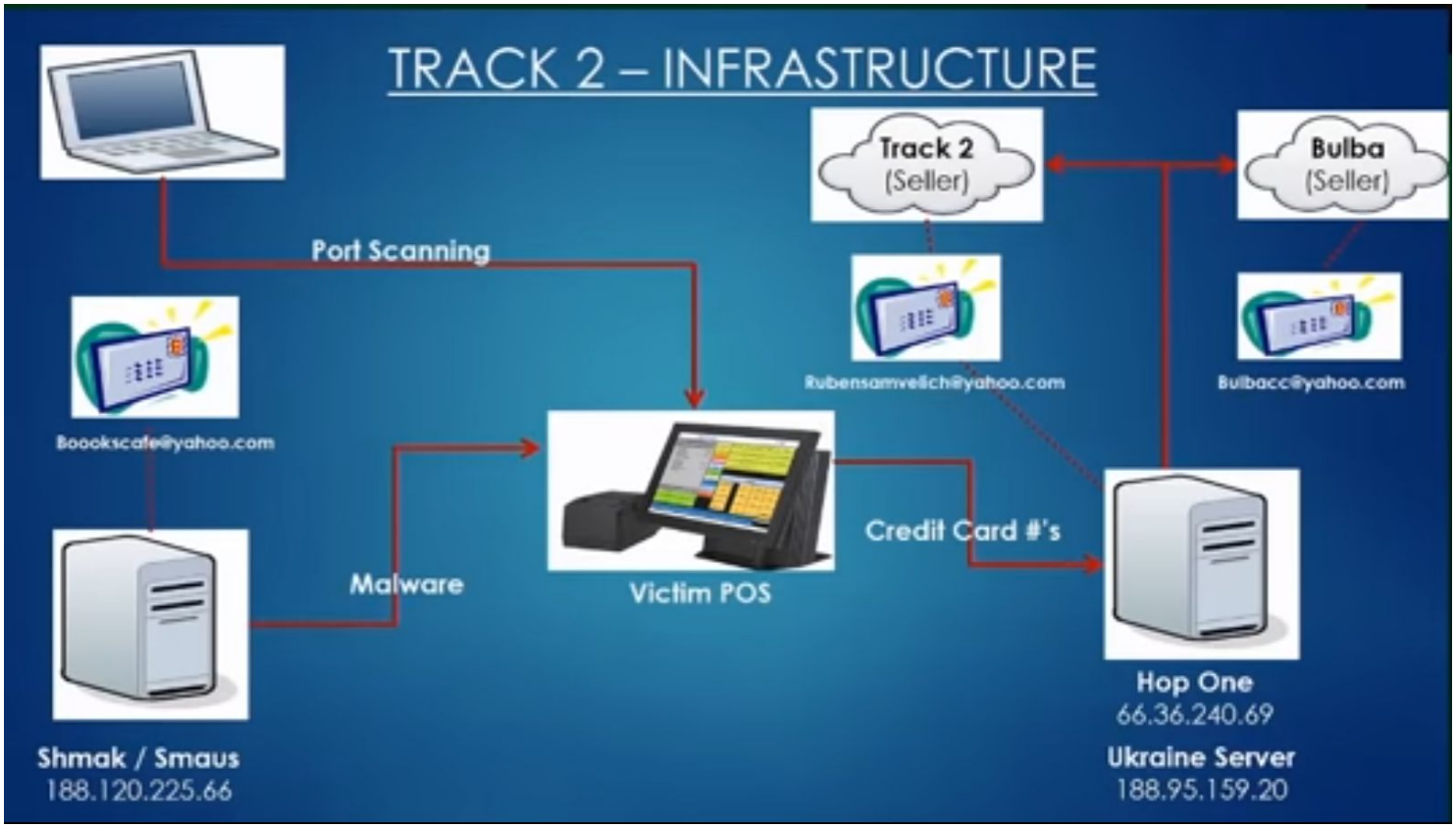
- Live in Russia
- Buy ransomware
  - Grancrab
- Rent/Buy infrastructure
- Buy creds to compromised systems
  - xdedic
- ??????
- Profit

Case Study - Roman Seleznev

- Russian carder
- Created webcrawler that looked for open 3389 port (RDP) and tried default creds
  - Look for financial data
  - Create and sell on carding forums and other DN markets
- Then focused on CC data and selling dumps on carder.su
- Compromised PoS systems in multiple restaurants in US
  - Feds identified CC fraud coming from some restaurants
  - Imaged PoS systems. Found connected to a C2 in McLean, VA
    - IP literally in browser history
  - Feds analyzed traffic to and from C2 to see other breached restaurant.

Case Study - Roman Seleznev

- Searching for 3389
  - RDP brute force
- Steal CC info, upload to 1 of 3 servers, stored based on originating IP



Case Study - Roman Seleznev

- Feds got access to email he used to register Track2 (seller) domain
  - WHOIS
  - Warrant for yahoo email
- Seleznev used it to open up a personal paypal account in his real name
- Feds got access to McLean C2 server
  - Seleznev used it to book personal flights with all his real passport info
    - Browser cache
- On a carding forum, Seleznev used his real name and address in a DM to another member who was arrested.
  - #opsec

Case Study - Roman Seleznev

- Flew through Korea on his way to second home in Indonesia
  - Stopped doing that before Feds could get to him.
- Started 2pac.cc
  - Created own market
  - Own dumps and dumps from others

Case Study - Roman Seleznev

- Flew through Korea on his way to second home in Indonesia
  - Stopped doing that before Feds could get to him.
- Started 2pac.cc
  - Created own market
  - Own dumps and dumps from others
  - Tutorials on how to buy dumps and use stolen CC's
- Flew to vacation in Maldives
  - No extradition treaty with US
  - Govt cooperated and Feds took him to Guam

- Feds got his laptop
  - ochko was on of his DN market usernames
  - Password to laptop was ochko123
  - 1.7million CC numbers on laptop

Case Study: Eldo Kim

- Harvard sophomore emailed bomb threats to Harvard
- Tor + Guerrilla Mail from Harvard wifi
- FBI interviews him, he confesses

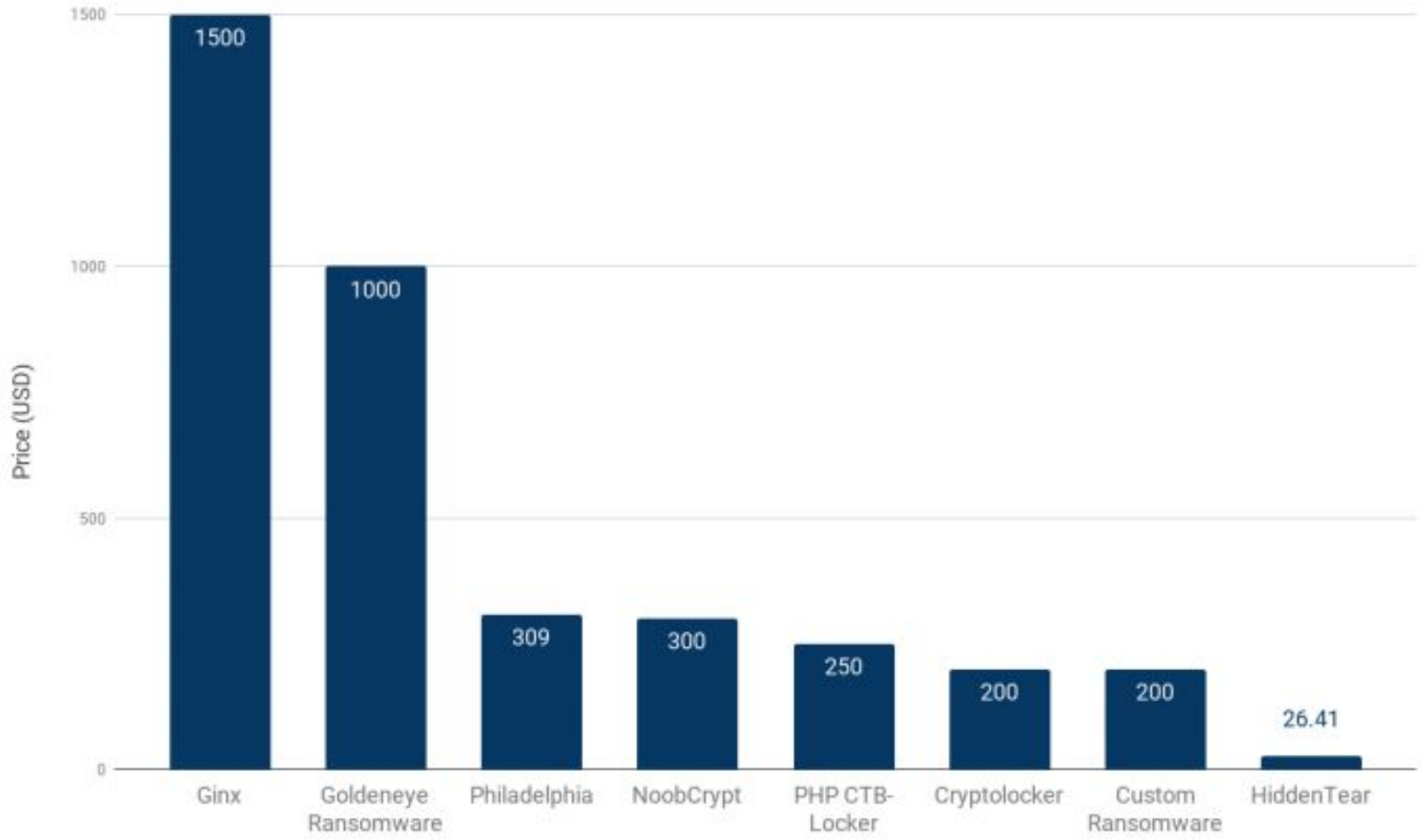
Top Darknet Markets

- Always get busted

Top English Ones

Silk Road → Silk Road 2.0 → Alphabay → Hansa → Dream Market

Fun Chart


Price (USD)
1500
1000
500
0
1500
1000
309
300
250
200
200
26.41
Ginx
Goldeneye Ransomware
Philadelphia
NoobCrypt
PHP CTB-Locker
Cryptolocker
Custom Ransomware
HiddenTear

Hidden Tear Tangent

- Intentionally flawed .NET ransomware
  - First open-source ransomware
  - Still gets some people
  - Wasn’t detect by AV on release date
- AES
  - Symmetric
- Encrypts files with key then sends key to “targetURL” via GET request

Hidden Tear Problems

- GET request in plaintext
  - Network logs FTW
- Pseudorandom encryption key more “pseudo” than “random”
  - Seed based on .Net’s Random() class based on Environment.TickCount
    - Number of milliseconds since computers last start
  - Last modified timestamp
  - One problem: small gap between last write and key gen
    - brute force, usually <50ms
      - » known file contents
      - » score
- IV reuse
- Static salt

Threat Intel

- Why is this info useful?

- Threat Intel sources
  - Blogs
  - Own research
- TI feeds = collection of sources
- Threat Intel Platforms
  - CRITS
  - YETI
  - MISP
- Data Format
  - STIX = format
  - TAXII = protocol for exchanging threat intel

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™