Financially-Motivated Cybercrime: The Turn to Intermediaries

Chris Jay Hoofnagle, Adjunct Professor, I School & Law
Aniket Kesari, JD/PhD Yale/Berkeley Student
Amanda Maya, JD Candidate
Damon McCoy, Assistant Professor, NYU CS & Engineering

Platform Law:
Public and Private Regulation of Online Platforms
April 20–21, 2017
Popular Perception: Cybercrime is anonymous, placeless

Source: FBI.gov
ECONOMIC ESPIONAGE

Deterring Financially Motivated Cybercrime

Zachary K. Goldman* & Damon McCoy**

Introduction

Deterrence is one of the most venerable concepts in the national security lexicon. It refers to the process of manipulating an adversary’s cost/benefit calculations to prevent him from doing something you do not want him to do. The concept is as old as warfare itself, reaching its apotheosis during the Cold War, when it was the central principle governing the security relationship between the United States and the Soviet Union.

But despite the pedigree of deterrence as a theory and a strategy, the community of scholars and practitioners focused on cybersecurity and cybercrime has struggled to adapt it to the burgeoning world of cyber threats. Admiral Michael Rogers, Director of the NSA, has said that the “fundamental concepts of deterrence” in cyberspace are “immature.” Senator John McCain has derided the “failure to develop a meaningful cyber deterrence strategy.” And some of the most prominent cybersecurity practitioners have noted that “deterrence is an undeveloped theoretical space in cyber war today.”

The cyber deterrence discussion has floundered thus far in part because of challenges that are unique to cyber space. This includes problems publicly attributing cyberattacks with confidence, the difficulty that inheres in determining whether a technological system has failed because of attack or for other reasons, and the unwillingness of states to discuss publicly capabilities that they treat as highly classified.

But part of the problem is also conceptual, derived from the fact that cyberattacks are motivated by an array of factors – cyber espionage is motivated

• “...for a particular spam network, just three acquiring banks managed the merchant accounts for 95% of the nearly 1 billion spam messages analyzed…”

• Cybercriminals may be difficult to reach, but their platforms are not

• Goldman & McCoy, Deterring Financially Motivated Cybercrime, 8 J. Nat’l Sec. L. & Pol’y 595 (2015-2016)

• Levchenko et al., Click Trajectories: End-to-End Analysis of the Spam Value Chain, Proceedings of the 2011 IEEE Symposium on Security and Privacy (2011)
Google Forks Over Settlement On Rx Ads

By Thomas Catan
August 25, 2011

WASHINGTON—In a rare public mea culpa, Google Inc. agreed to pay $500 million to avoid Justice Department prosecution on charges that it knowingly accepted illegal advertisements from Canadian online pharmacies for years.
Google agrees to anti-pharma ad procedures
Thus phar... a compete in organic search

Sponsored: no illegal pharma

Okay to have in organic results
How to get to the top?
Collect top-ranked results

Link analysis of ads, html links, customer service, payment in Palantir Gotham
For Platform Law: How Do Enforcers Use the Law to Police Intermediaries?

- Botnets, hacking for hire
- Transnational criminal organizations
- Counterfeit goods
- Anti-prostitution
Interventions: Rule 65 TROs & FCRMP 41

- Standard Rule 65 TRO, PIs used for
  - Anti-botnet activities
  - Counterfeiting
- Relief is granted quickly—sometimes within days
- Relief includes seizures of scores of domain names
- Ex parte
- In new Kelihos botnet, gov’t relied on FCRMP 41
  - But procedure looks the same—
  - Gov’t identifies, seizes command & control servers
  - “Sinkholes” communications or patches vulnerable bots
Interventions: Treasury Sanctions

- Department of Treasury’s Specially Designated Nationals List is being used to block transactions with cyber actors.
- These are asset blocks, bans on US companies doing business with designated individuals
- 3 programs being used:
  - Cyber: No one yet designated.
    - EO 13694 (Obama 2015)
  - Cyber2: Russian operation related to 2016 election hacking.
    - EO 13757 (Obama 2016)
  - TCO: PacNet group money laundering.
    - Transnational Criminal Organizations Sanctions Regulations, Executive Order 13581
Interventions: Payment Systems

• These are both private and public interventions
• Operation Chokepoint
• Self-regulatory efforts
  • Amex (closed loop system) attempting to cut off Backpage.com ("escort" services)
  • CA AG’s money laundering case against Backpage stands atop efforts to circumvent Amex’s ban
Concluding

• CDA & DMCA is a focus of the legal literature of intermediaries
• But our work focuses on other interventions
• We’ll discuss claimant abuse, due process, overbreadth
• We suspect intermediary attacks will continue to be effective against financially-motivated cybercriminals, especially when payment platforms are targeted
  • Too many alternatives in the DNS space; whack-a-mole
  • Google will continue to be a key intermediary
  • Decentralization of service providers (e.g. BitCoin) is an unlikely alternative
Thanks to...

- Center for Long-Term Cybersecurity
- Palantir Technologies
- Laurin Weissinger, Nuffield