Cybereconomics

Stefan Savage

UCSDCSE
Computer Science and Engineering

Security is a social science

- There is a technical component, no doubt, but…
- Fundamental non-technical components drive real life outcomes
  - Behavior
  - Motivations
  - Relationships
  - Incentives
  - Perception
  - Value
- You have to model *these things* to model security impact

Two sides of cybereconomics

Defender

Cost centers

Return on Investment

Incentives

Adversary

Profit centers

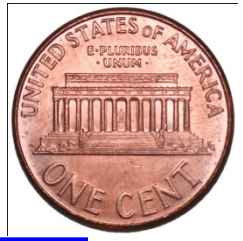
Return on Investment

Disincentives

Economics of defense

- Outcomes depend on three things
  - User behavior
  - Attacker behavior
  - Defender behavior
- Things about outcomes we **don't** know, but ***could*** know
  - How much does it matter if you have good "Internet hygiene"?
  - How much does it matter if you patch your systems?
  - What kinds of users/systems attract the most attacks?
  - How much does it matter if you run AV and for what?
  - How much does it matter if you do quick incident response?
  - What's the best way to stop phishing: mail filters, browser blacklists or takedowns?
- **Evidence-based security**

Offence via economics



- Adversaries increasingly have a complex value chain
  - E.g. spam-based advertising: hosting, registrar, payment processing, affiliate program, malware author, botnet operator, compromised hosts, proxy network, etc…
  - We largely ignore it today
- To build the most efficient defenses, we need to understand the attacker's cost structure and value
- To maximize impact to adversary, need to target the most valuable part of their value chain

Example: CAPTCHAs

- Current **retail** cost to solve 1,000 CAPTCHAs?

- Wholesale cost can be half that…

Example: compromised hosts

- Current **retail** cost to get 1,000 compromised hosts?

- For Asia… western hosts up around $100/1000

Installs4Sale.net - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://installs4sale.net/

Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Pr

Google Search Sidewiki Bookmarks Translate AutoLink

Installs4Sale.net

WebMoney

- Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
- Мы отслеживаем уникальность инсталов и их чистоту перед продажей.

УСЛОВИЯ

- Мы работаем строго по предоплате. Допускается частичная оплата постоянным клиентам на большие объемы.
- Мы не несем ответсвенности за то что у вас по каким-то причинам отстувуют загрузки. Если вы не видите инсталов с первых минут мы можем проистановить отгрузку до выяснения обстоятельств.

ТАРИФЫ

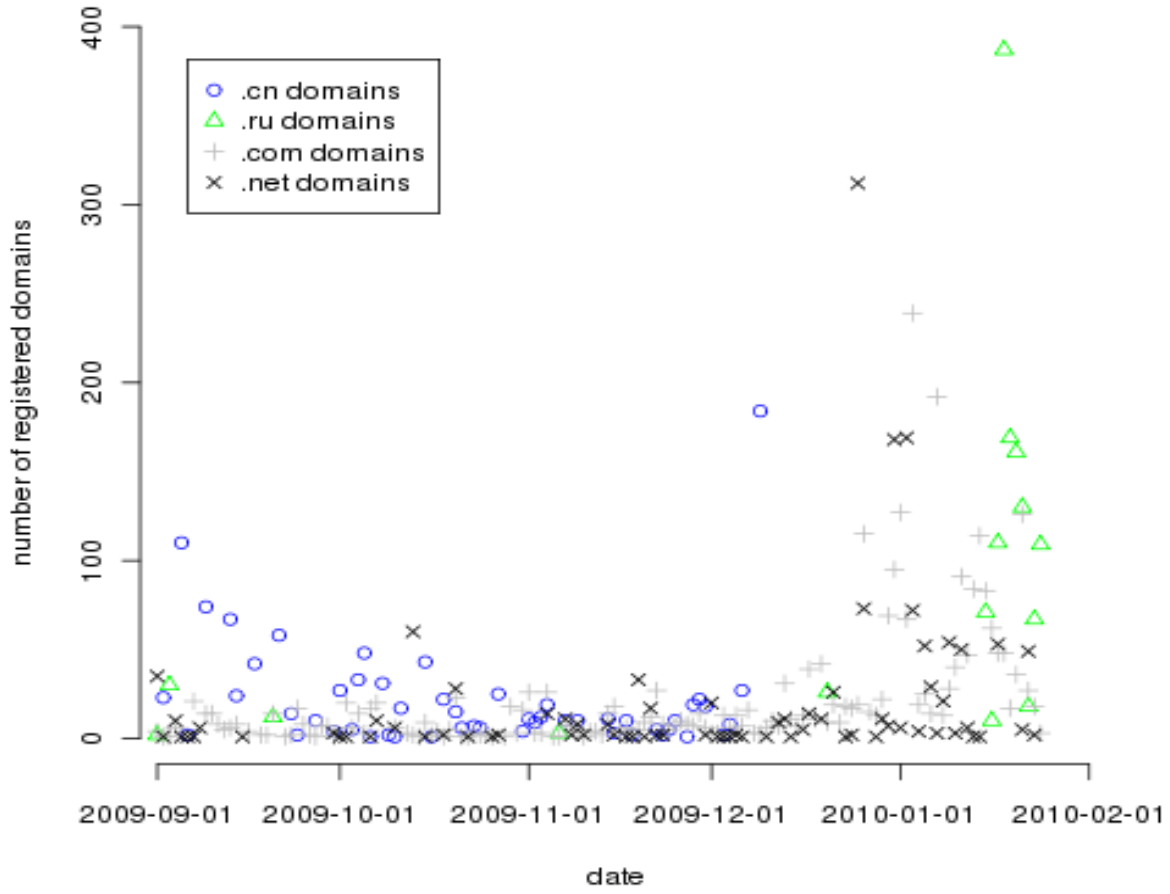
GB (Англия)	150$
DE (Германия)	150$
USA (США)	130$
IT (Италия)	120$
Микс (US,CA, AU, GB)	100$
CA (Канада)	100$
Микс (Европа)	40$
Азия	10$

Все цены указаны за 1000 уникальных загрузок

Все права защищены installs4sale.net. 2009

Example: domain names

- Cost depends… and it matters (e.g., for spam)



A research agenda going forward

- Users and defenders
  - Experimentally determine which technology, processes, behaviors, etc are producing which outcomes
  - Explore how to incentivizes the best of these

- Attackers
  - Measure or infer value chain, business relationships, cost basis of today's adversaries
    (and technology to support such measurement)
  - Determine set of "weakest links" (most valuable, least adaptable, etc) that can be most cheaply targeted