Worms, Botnets and The Underground Economy

CS 161 - Computer Security

Profs. Vern Paxson & David Wagner

TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger

http://inst.eecs.berkeley.edu/~cs161/

April 16, 2010

Further Worm Developments

- Malicious payloads (disk-trashing)
- Global outbreaks within 24 hours of vulnerability disclosure
- "Server" exploited for infection is a NIDS
- Single outbreak of > 15 million infectees
- "*Counterworm*" released to clean up original worm …
  - … oh and install a root backdoor
- DoS'ing *Windows Update* as a worm spreads
- Worms that use Google to search for victims

Thinking About Worm Defenses

- We can methodically explore possible worm defenses by considering $\frac{dI(t)}{dt} = \beta \cdot I(t) \cdot \frac{S(t)}{N}$
- Strategy #1: reduce contact rate β to slow a worm's propagation …
- … how can we reduce it?
  - Decrease N so that random scanning less effective
    - Turn off unneeded services; aggressive patch management
  - Increase size of address space (IPv6)
    - Worm countermeasures?
      - Heuristics to guess likely address use patterns
      - Locate likely victims via DNS, Google
  - Suppress scans (limit connection "fanout")
  - Isolate susceptibles (install firewall blocks upon outbreak)

Thinking About Defenses, con't

$$\frac{dI(t)}{dt} = \beta \cdot I(t) \cdot \frac{S(t)}{N}$$

- Reduce I(t)
  - Identify and isolate ("quarantine") infected hosts
- Reduce S(t)
  - Dynamically push out patches

- What did Slammer teach us about employing dynamic defenses?
  - They have to be fully automated
    - No human in the loop
  - Thus: highly accurate

Worm Take-Aways

- Potentially enormous reach/damage
  ⇒ *Weapon*
- Hard to get right
- Emergent behavior / surprising dynamics
- Institutional antibodies
- *Propagation faster than human response*

- What about fighting a worm using a worm?
  - "White worm" spreads to disinfect/patch
  - Experience shows: likely not to behave predictably!
  - Additional issues: legality, collateral damage, target worm having already patched so white worm can't access victim

Botnets

- Collection of compromised machines (bots) under (unified) control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm / virus / drive-by infection / etc.
- Upon infection, new bot "phones home" to rendezvous w/ botnet command-and-control (**C&C**)
- Lots of ways to architect C&C:
  - Star topology; hierarchical; peer-to-peer
  - Encrypted/stealthy communication
- Botmaster uses C&C to push out commands and updates

Botnets, con't

- Constitute the *Great Modern Threat* of Internet security
- Why botnets rather than worms?
  - Greater control
  - Less emergent
  - Quieter
  - Optimal flexibility
- Why the shift towards valuing these instead of seismic worm infection events?

  $$ Profit $$
- How can attackers leverage scale to monetize botnets?

Monetizing Botnets

- General malware monetization
  - Keylogging: steal financial/email/social network accounts
  - Transaction generators
- Monetization that leverages scale
  - DDoS (extortion)
  - Spam (discussed next week)
  - *Click fraud*
  - Scam infrastructure
    - Hosting web pages (e.g., phishing)
    - Redirection to evade blacklisting/takedown (DNS)
- Which of these cause serious pain for infected user?
  - **None**. Users have little incentive to prevent ($\Rightarrow$ ***externality***)

Original URL: http://www.theregister.co.uk/2010/03/03/mariposa_botnet_bust_analysis/

How FBI, police busted massive botnet

12m zombie machines run by 3 admins

By **John Leyden**

Posted in Malware, 3rd March 2010 15:56 GMT

Analysis More details have emerged about a cybercrime investigation that led to the takedown of a botnet containing 12m zombie PCs and the arrest of three alleged kingpins who built and ran it.

As previously reported, the Mariposa botnet was principally geared towards stealing online login credentials for banks, email services and the like from compromised Windows PCs. The malware infected an estimated 12.7 million computers in more than 190 countries.

The Mariposa Working Group infiltrated the command-and-control structure of Mariposa to monitor the communication channels that relayed information from compromised systems back to the hackers who run the botnet. Analysis of the command system laid the groundwork for the December 2009 shutdown of the botnet, as well as shedding light on how the malware operated and provided a snapshot of the current state of the underground economy.

The botmasters made money by selling parts of the botnet to other cybercrooks,

Netkairo finally regained control of Mariposa and launched a denial of service attack against Defence Intelligence using all the bots in his control. This attack seriously impacted an ISP, leaving numerous clients without an Internet connection for several hours, including several Canadian universities and government institutions.

Once again, the Mariposa Working Group managed to prevent the DDP Team from accessing Mariposa. We changed the DNS records, so the bots could not connect to the C&C servers and receive instructions, and at that moment we saw exactly how many bots were reporting. We were shocked to find that more than 12 million IP addresses were connecting and sending information to the C&C servers, making Mariposa one of the largest botnets in history.

alleged lieutenants “Ostiator” and “Johnyloleante” have been charged with cybercrime offences. More arrests are expected to follow.

Under Spanish law suspects are not named at this stage of proceedings. Pedro Bustamante, senior research advisor at Panda Security, said: “Our preliminary analysis indicates that the botmasters did not have advanced hacking skills.

"This is very alarming because it proves how sophisticated and effective malware distribution software has become, empowering relatively unskilled cyber criminals to inflict major damage and financial loss." ®

Spy Instructors Software

NEW GENERATION SOFTWARE SOLUTIONS

HOMEPAGE | PRODUCTS | DOWNLOADS | FORUMS | ABOUT US

ProAgent v2.1

- ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.
- It is an ultimate solution for monitoring spouses, children, employees, or anyone else!
- ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!
- ProAgent can work in all kind of networks, it doesn't matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase **ProAgent v2.1** Special Edition...

Click here to download **ProAgent v2.1** Public Edition

SIS - Products

Purchase Program

Customer Support Department

Commercial Programs

Freeware Programs

Custom Special Programs

New Generation Software Solutions...

New Products

SIS-IExploiter v2.0

ProAgent v2.1

AntiDote v1.2

SIS-Downloader

Virtual Keyboard

Список доступных акков

Сервис по продаже аккаунтов аукцыона eBay.

Добрые юзеры аукцыона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
Все аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субьективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гарант сервис приветствуется.

Мои цены:

seller/баер акк до 10 фидов = 5$
seller/баер акк 10-25 фидов = 10$
seller/баер акк 25-50 фидов = 15$
seller/баер акк более 50 фидов = 25$

allBots Inc.

Social Networking Bots

GOOD News!!! We have something more for you! Yes, we have just integrated **CAPTCHA Bypasser**** in all of our bots.

Winsock (Multi-threaded) Bots

Become an Affiliate and Start Earning Now

Click here for 30+ MySpace Bots

Accounts Creator

(You Just Need To Type In The CAPTCHAs To Create Accounts)

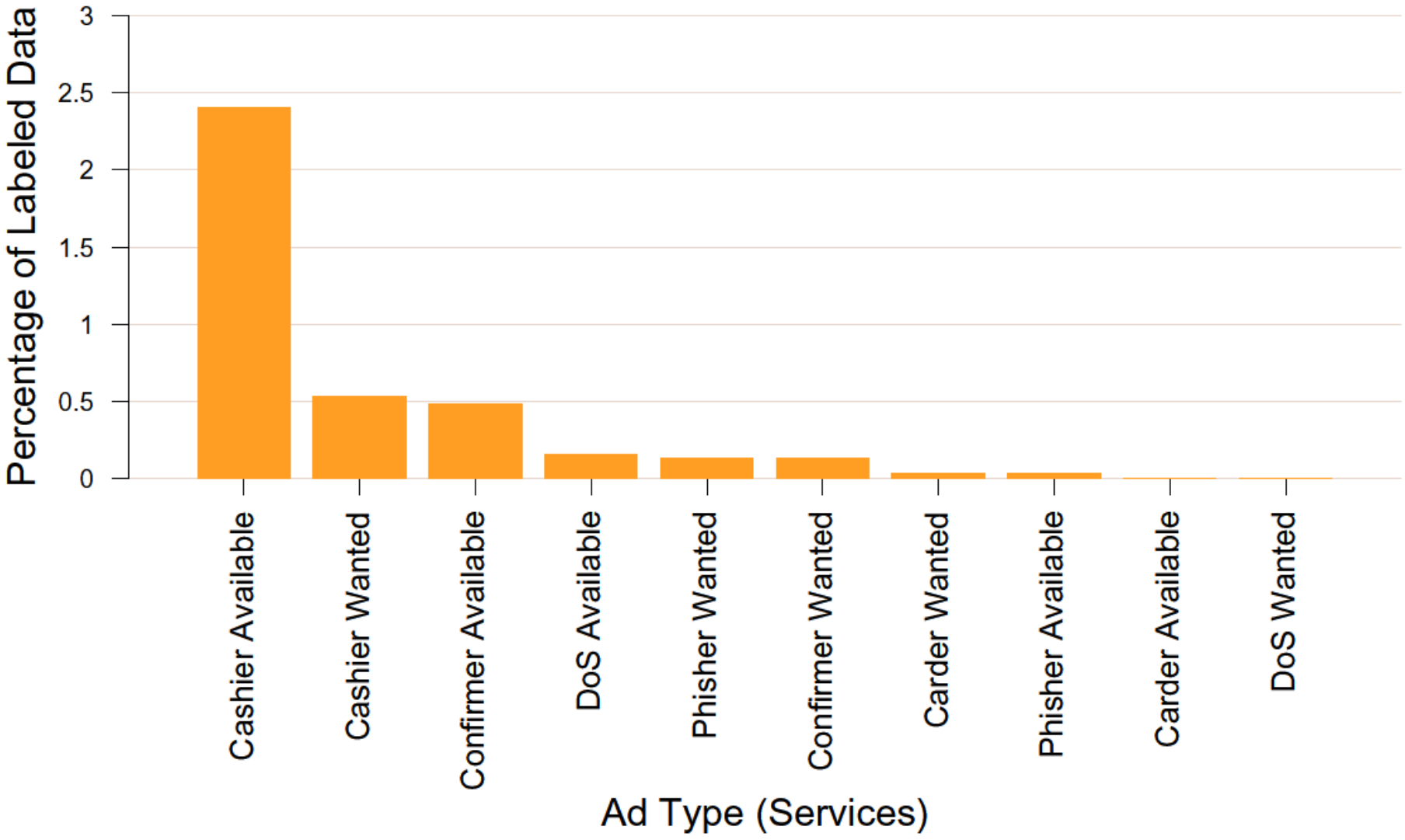
Social Networks			
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager	PayPal Buy Now	~~$180.95~~	$140.00
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)	PayPal Buy Now	~~$360.95~~	$320.00
YouTube Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Friendster Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Hi5 Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
TagWorld Accounts Creator	PayPal		

Friend Adders, Message Senders, Comment Posters & Others

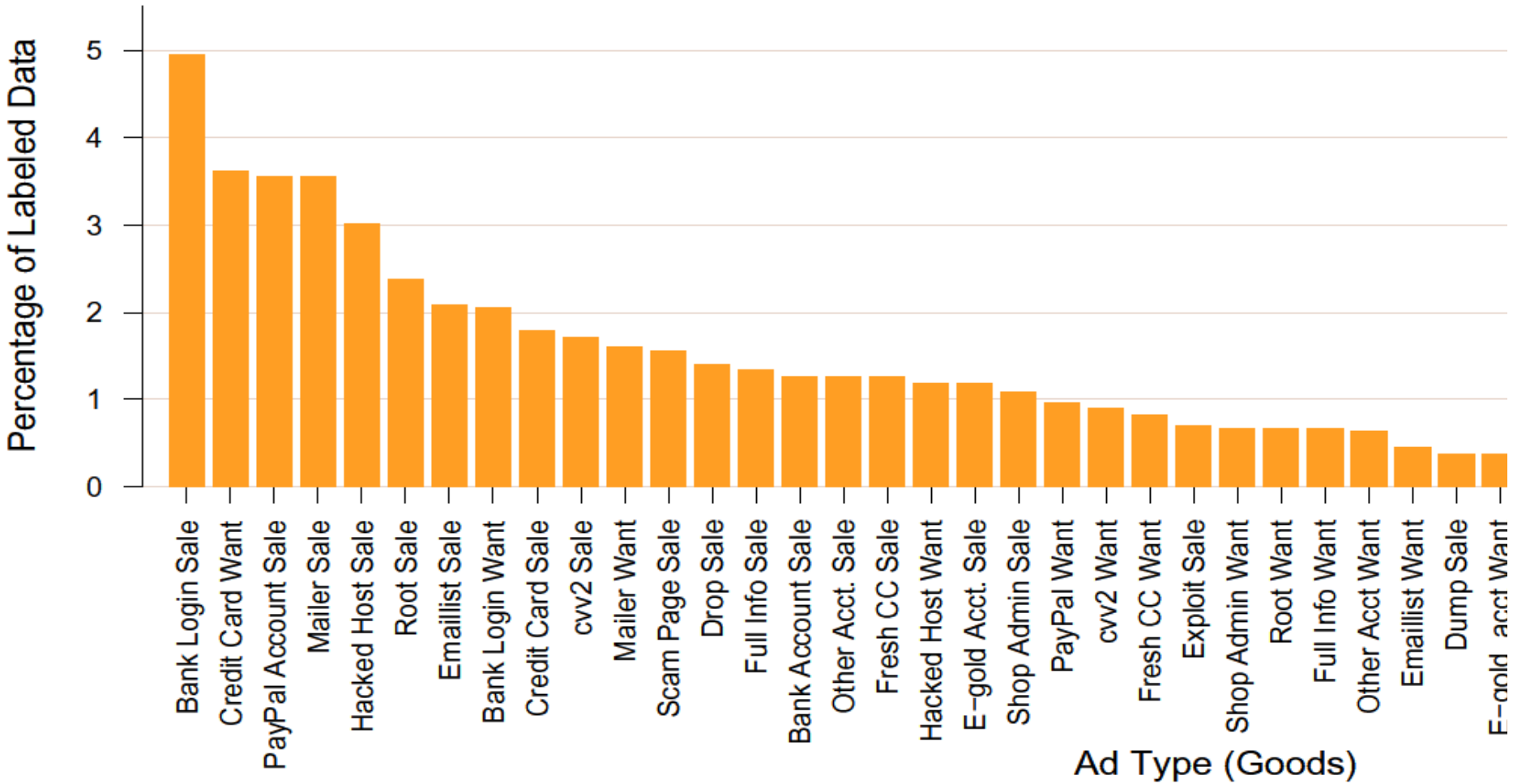
(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)

Chaining Feature Is Available On All Bots for All Networks Except Facebook

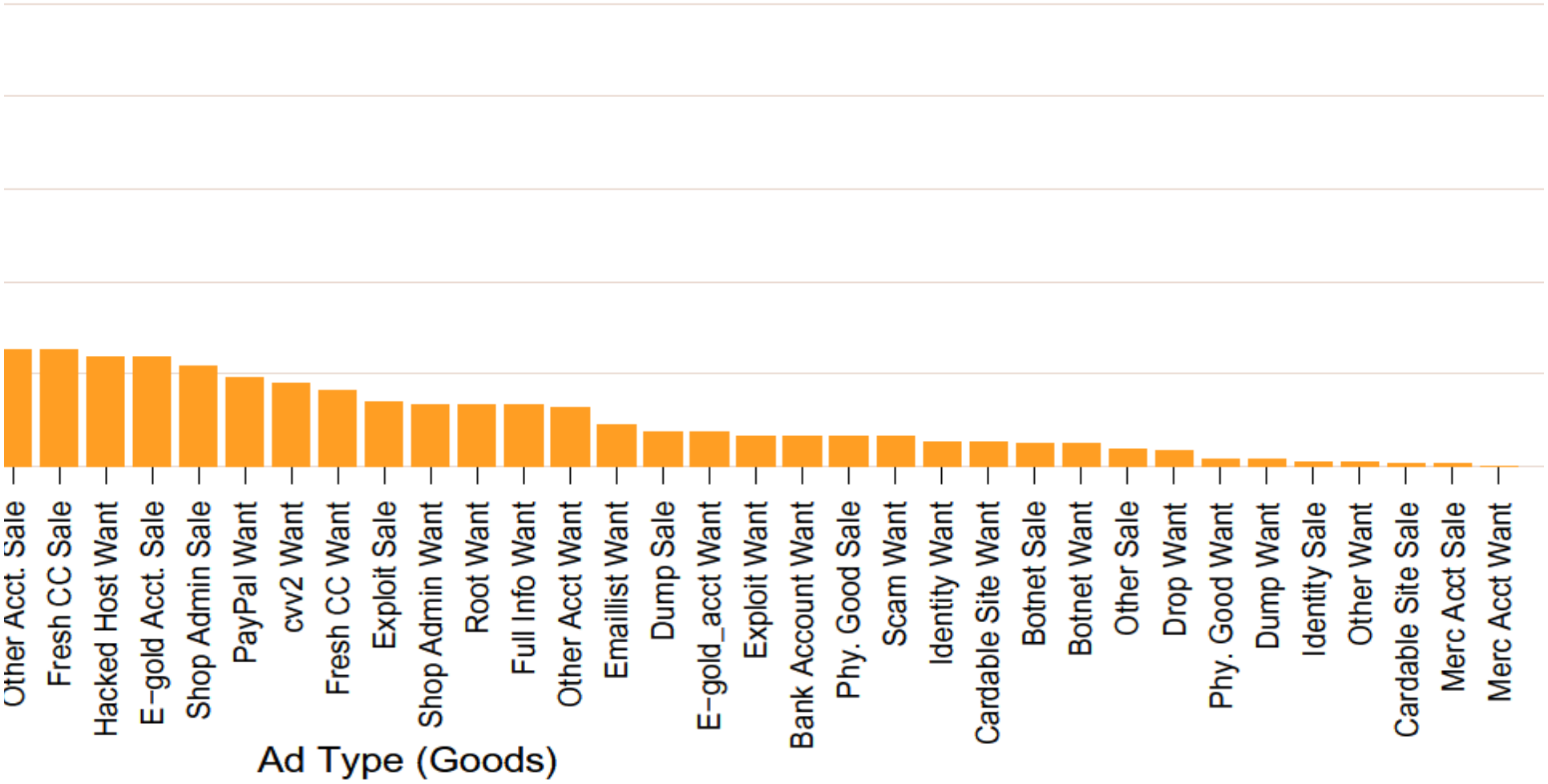
Marketplace Ads for Services



Marketplace Ads for Goods



Marketplace Ads for Goods, con't



The Underground Economy

- Why is its emergence significant?

- Markets enable efficiencies
  - *Specialization*: individuals rewarded for doing a single thing particularly well
- Lowers barrier-to-entry
  - Only need a single skill
  - Some underground market activities are legal
- Competition spurs *innovation*
  - Accelerates **arms race**
  - Defenders must assume a more pessimistic threat model
- Facilitates non-$ Internet attacks (political, nation-state)
  - Provides actors with cheap attack components
  - Provides stealthy actors with plausible cover

The Underground Economy, con't

- What problems do underground markets face?
- Markets only provide major efficiencies if they facilitate deals between strangers
  - Susceptible to *infiltration*
- Depending on marketplace architecture, can present a target / single point of failure
- By definition, deals are between **crooks**
  - Major issue of betrayal by "*rippers*"