CSE 484 / CSE M 584
Computer Security:

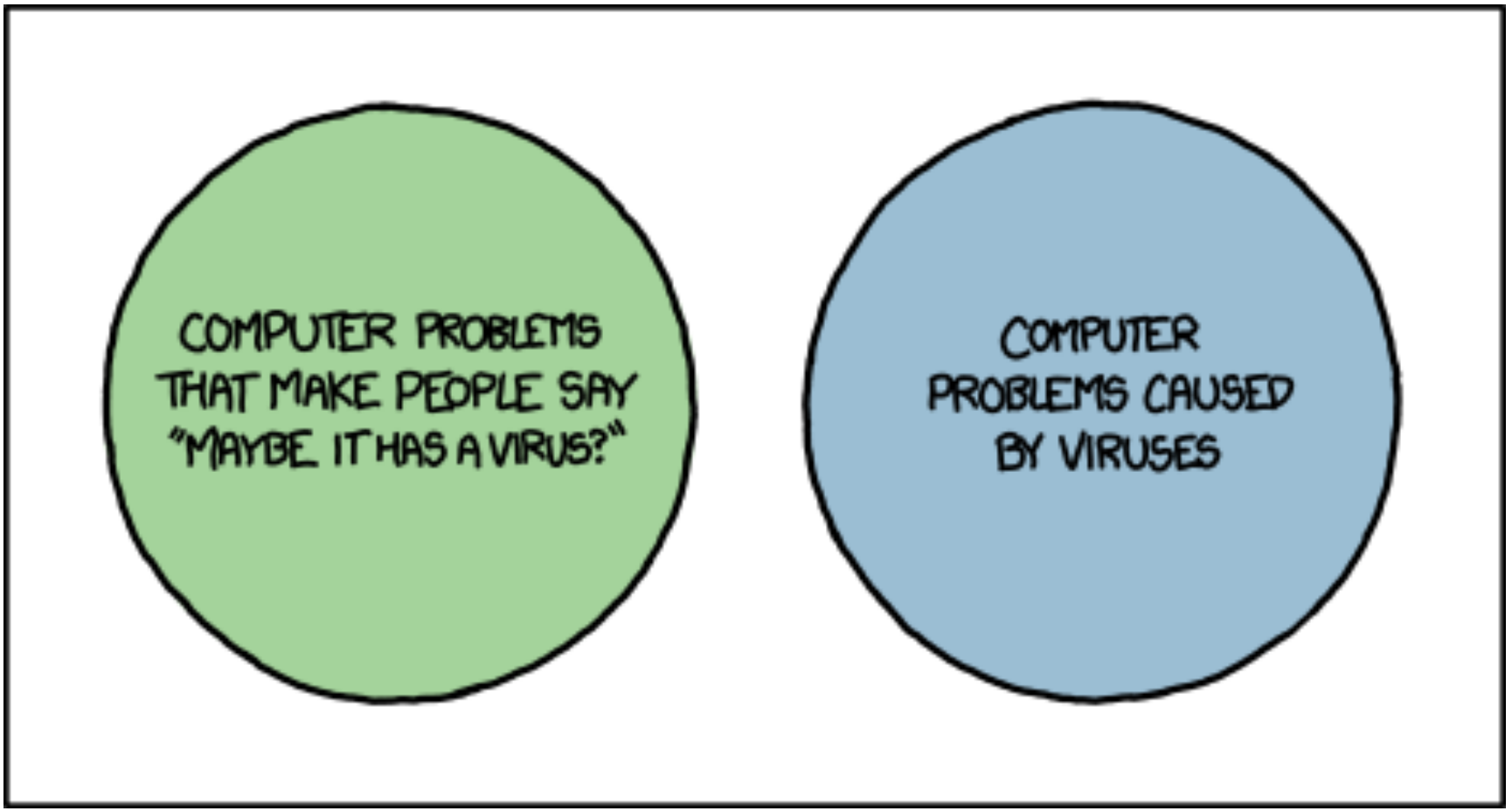
Malware and
Online Ecosystem Studies

TA: Thomas Crosley
tcrosley@cs
With material from Franzi, Adrian Sham, and various sources

Reminders

- Homework #3, due May 23th, 8pm (Tomorrow!)
- Lab #3 due June 3, 8pm
- Preliminary Final Project Due Date #2
  - (This!) Monday May 30th, 8pm

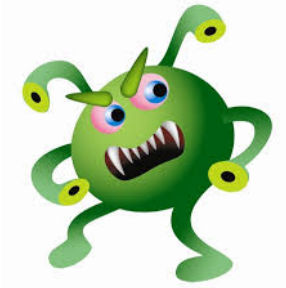
Malware


COMPUTER PROBLEMS THAT MAKE PEOPLE SAY "MAYBE IT HAS A VIRUS?"
COMPUTER PROBLEMS CAUSED BY VIRUSES

Malware

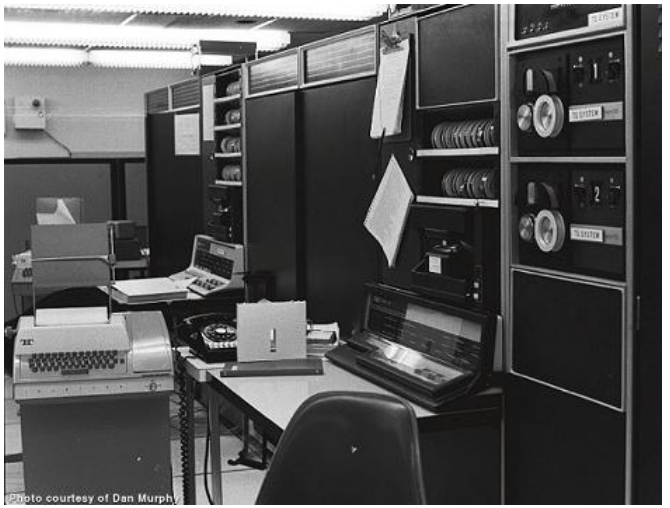
- Malicious code often masquerades as good software or attaches itself to good software
- Some malicious programs need host programs
  - Trojan horses (malicious code hidden in useful program)
- Others can exist and propagate independently
  - Worms, automated viruses
- Many infection vectors and propagation methods
- Modern malware often combines techniques

Viruses



- Virus propagates by infecting other programs
  - Automatically creates copies of itself, but to propagate, a human has to run an infected program
  - Self-propagating viruses are often called worms
- Many propagation methods
  - Insert a copy into every executable (.COM, .EXE)
  - Insert a copy into boot sectors of disks
    - PC era: "Stoned" virus infected PCs booted from infected floppies, stayed in memory, infected every inserted floppy
  - Infect common OS routines, stay in memory

First Virus: Creeper



- Written in 1971 at BBN
- Infected DEC PDP-10 machines running TENEX OS
- Jumped from machine to machine over ARPANET
  - Copied its state over, tried to delete old copy
- Payload: displayed a message
  "I'm the creeper, catch me if you can!"
- Later, Reaper was written to delete Creeper

http://history-computer.com/Internet/Maturing/Thomas.html

Virus Detection

- Simple anti-virus scanners
  - Look for signatures (fragments of known virus code)
  - Heuristics for recognizing code associated with viruses
    - Example: polymorphic viruses often use decryption loops
  - Integrity checking to detect file modifications
    - Keep track of file sizes, checksums, keyed HMACs of contents

Arms Race: Polymorphic Viruses

- Encrypted viruses: constant decryptor followed by the encrypted virus body
- Polymorphic viruses: each copy creates a new random encryption of the same virus body
  - Decryptor code constant and can be detected
  - Historical note: "Crypto" virus decrypted its body by brute-force key search to avoid explicit decryptor code

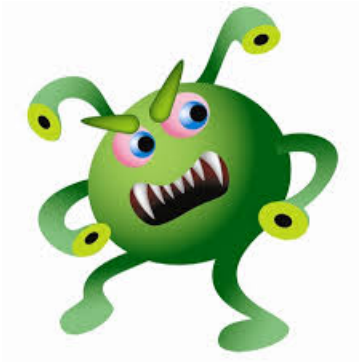
Smarter Virus Detection?

- Generic decryption and emulation
  - Emulate CPU execution for a few hundred instructions, recognize known virus body after it has been decrypted
  - Does not work very well against viruses with mutating bodies and viruses not located near beginning of infected executable

Viruses vs. Worms

VIRUS

- Propagates by infecting other programs
- Usually inserted into host code (not a standalone program)



WORM

- Propagates automatically by copying itself to target systems
- A standalone program

Slammer (Sapphire) Worm

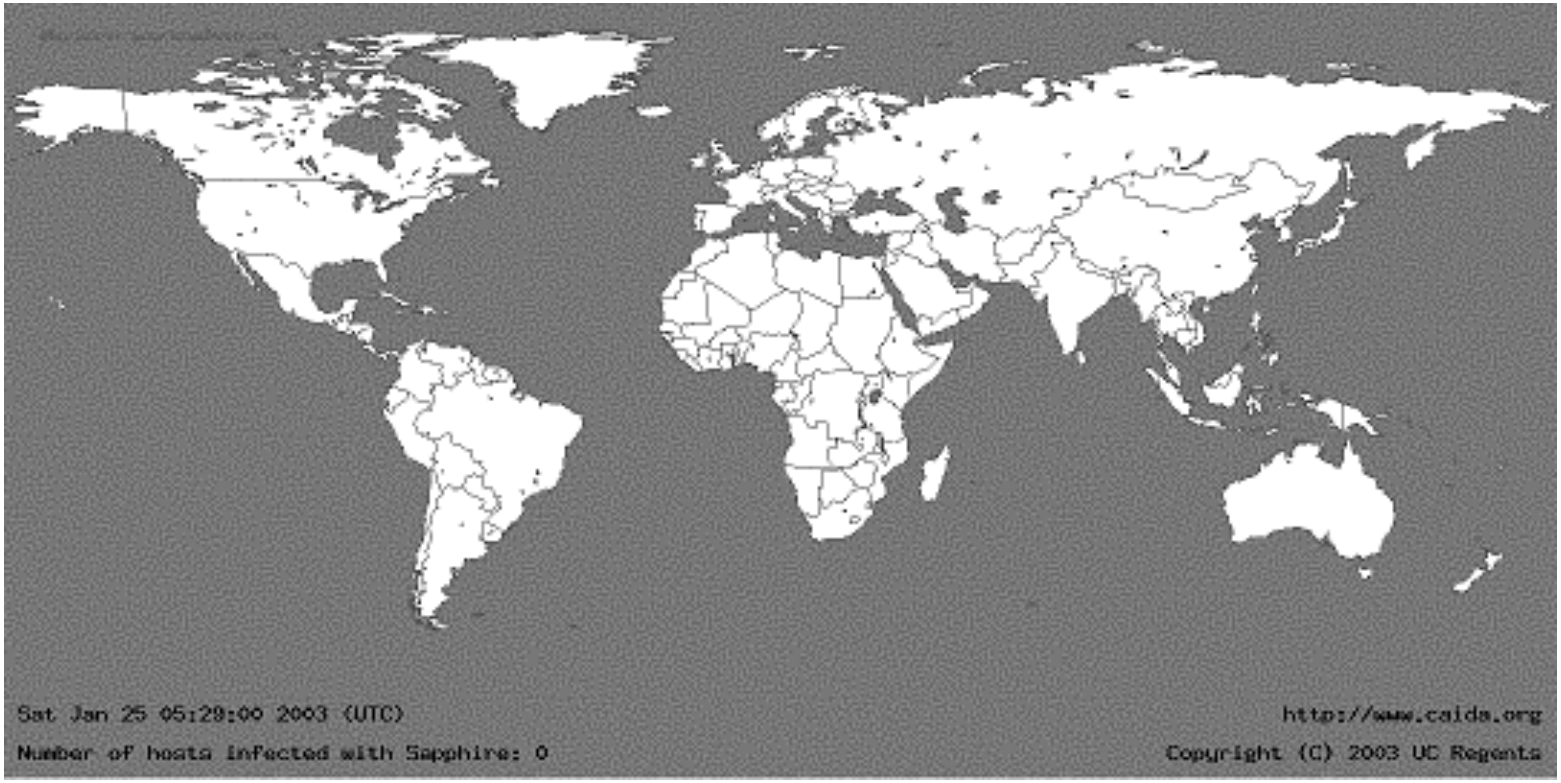
- January 24/25, 2003: UDP worm exploiting buffer overflow in Microsoft's SQL Server (port 1434)
  - Overflow was already known and patched by Microsoft… but not everybody installed the patch
- Entire code fits into a single 404-byte UDP packet
  - Worm binary followed by overflow pointer back to itself
- Classic stack smash combined with random scanning
  - Once control is passed to worm code, it randomly generates IP addresses and sends a copy of itself to port 1434

Slammer Propagation

- Scan rate of 55,000,000 addresses per second
  - Scan rate = the rate at which worm generates IP addresses of potential targets
  - Up to 30,000 single-packet worm copies per second
- Initial infection was doubling in 8.5 seconds (!!)
  - Doubling time of Code Red (2001) was 37 minutes
- Worm-generated packets saturated carrying capacity of the Internet in 10 minutes
  - 75,000 SQL servers compromised
  - … in spite of the broken pseudo-random number generator used for IP address generation

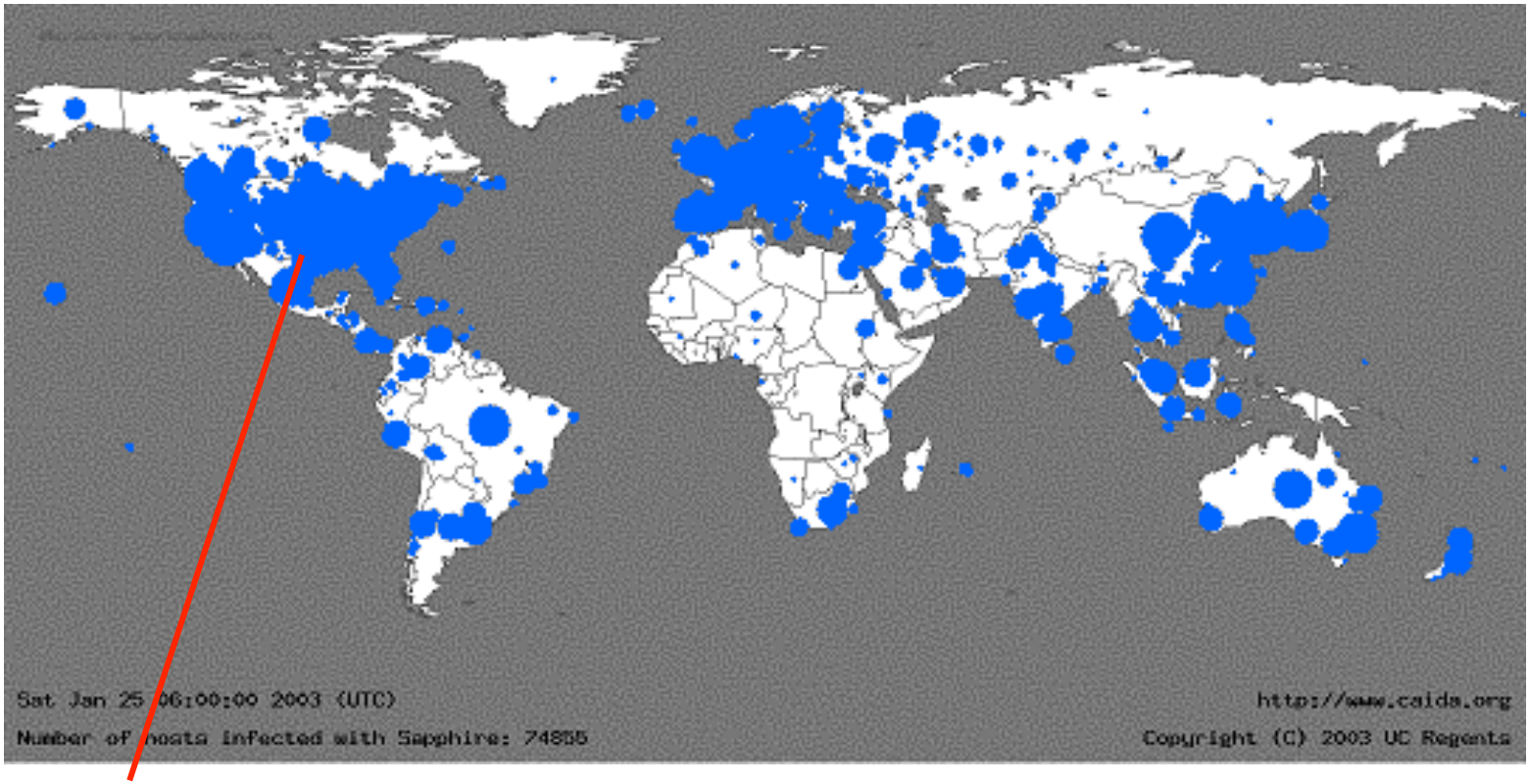
05:29:00 UTC, January 25, 2003

[from Moore et al. "The Spread of the Sapphire/Slammer Worm"]



30 Minutes Later

[from Moore et al. "The Spread of the Sapphire/Slammer Worm"]



Size of circles is **logarithmic** in the number of infected machines

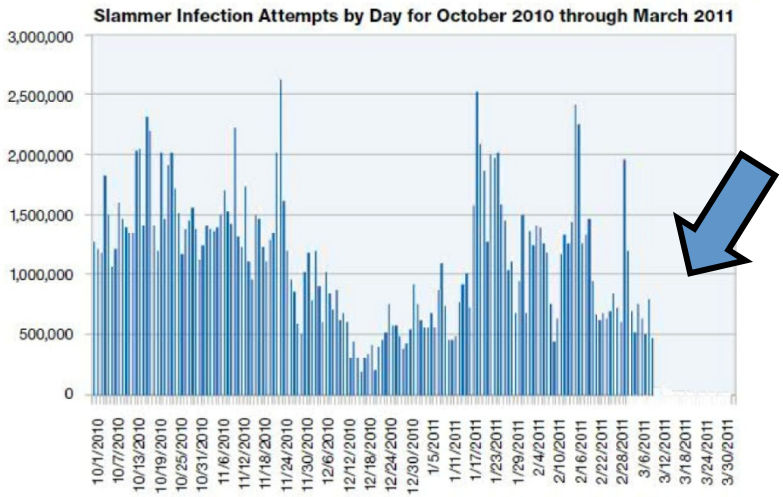
Impact of Slammer

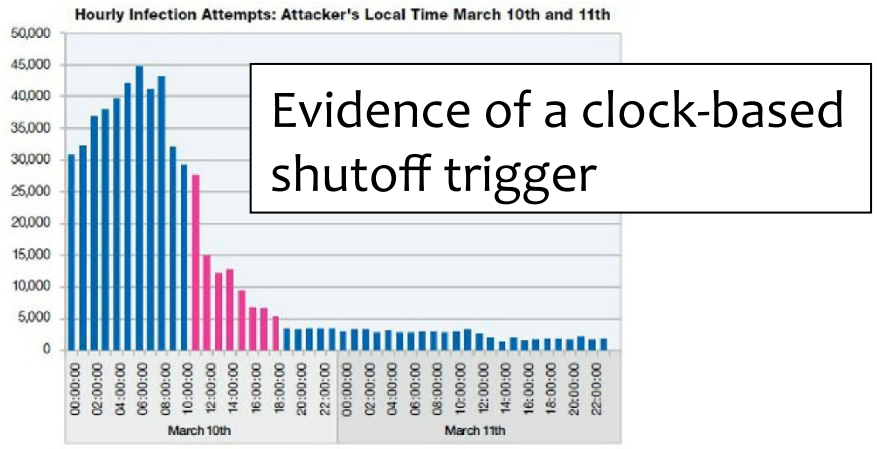
- $1.25 Billion of damage
- Temporarily knocked out many elements of critical infrastructure
  - Bank of America ATM network
  - Entire cell phone network in South Korea
  - Five root DNS servers
  - Continental Airlines' ticket processing software
- The worm did not even have malicious payload… simply bandwidth exhaustion on the network and CPU exhaustion on infected machines

[Cross and Valacek]

Slammer Aftermath

- Slammer packets were ubiquitous in the Internet for many years after 2003
  - Could be used as a test for Internet connectivity ☺
  - Packets provided a map of vulnerable machines
- Vanished on March 10-11, 2011





Evidence of a clock-based shutoff trigger

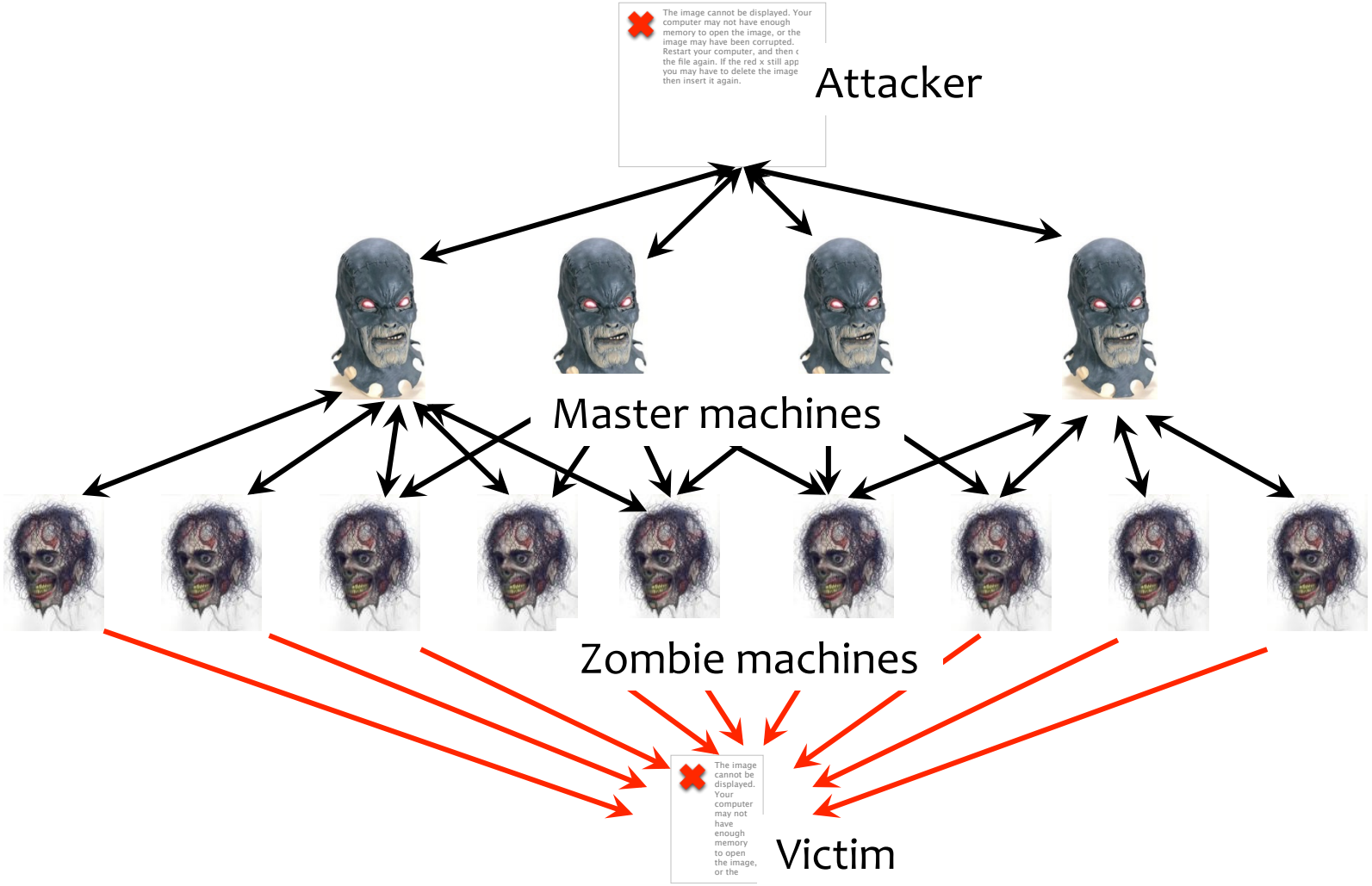
Botnets

- Botnet is a network of autonomous programs capable of acting on instructions
  - Typically a large (up to several hundred thousand) group of remotely controlled "zombie" systems
    - Machine owners are not aware they have been compromised
  - Controlled and upgraded from command-and-control (C&C) servers
- Used as a platform for various attacks
  - Distributed denial of service, Spam and click fraud
  - Launching pad for new exploits/worms

What to Do With a Botnet?

- Denial of service (including cyber-warfare)
- Spam
- Fake antivirus sales, Ransomware
- Advertising clickfraud
- Bitcoin mining
  - According to Symantec, one compromised machine yields 41 US cents a year…

Distributed Denial of Service (DDoS)



How to Protect Yourself?

- Nothing is perfect but…
  - Keep your software updated
  - Be vigilant for phishing attacks
  - Anti-virus
  - Firewalls
  - Intrusion detection systems

Online Ecosystem Studies

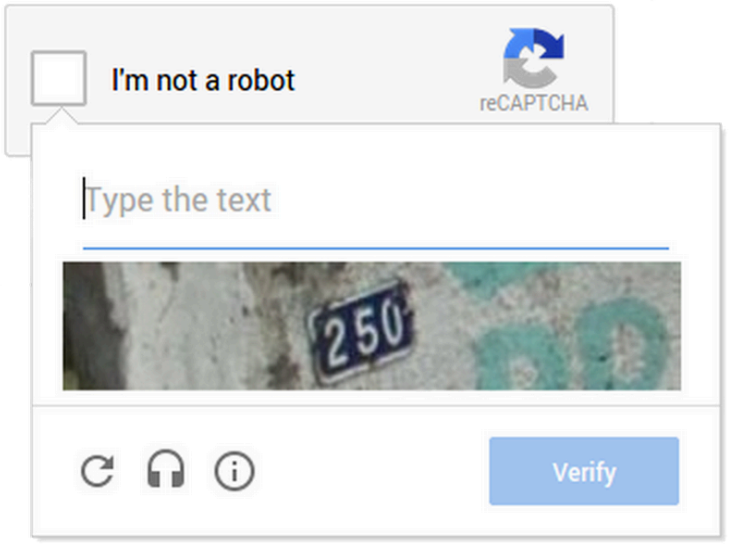
CAPTCHA

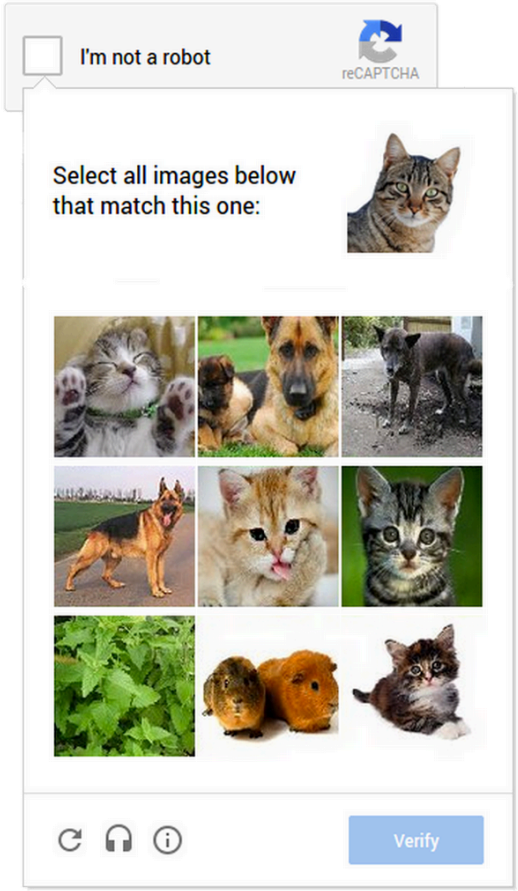
- CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part)
- Artificial Intelligence technology can solve 99.8%

http://googleonlinesecurity.blogspot.com/2014/12/are-you-robot-introducing-no-captcha.html

reCAPTCHA

- Use risk analysis, provide better user experience





[Motoyama et al.]

Dirty Jobs – The Role of Freelance Labor in Web Service Abuse

Following slides by : Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker UC San Diego

https://www.usenix.org/legacy/events/sec11/tech/slides/motoyama.pdf

[Motoyama et al.]

Vulnerability of Web Services

- Many web services today are free/open access
  - Supported by advertising revenue
  - Reaching critical mass requires low barrier to entry
  - Page views driven by user-generated content
    - Videos, social networking updates, blogs, etc
- However, openness leaves sites vulnerable to abuse
  - Exploitation of free resources
    - Sending spam from web based email accounts
  - Unsanctioned advertising channels
    - Spamming links on blog comments

[Motoyama et al.]

Abuse Labor Markets

- Abuse is profitable
  - Kanich et al. estimated $7k/day email spam revenue
- Labor markets have evolved to supply workers
  - Online freelancing sites
- Why outsource abuse jobs?
  - Cost effective: Low wage regions
  - Agile: Workers are adept and technically capable
  - Scale: ~one million workers on Freelancer.com

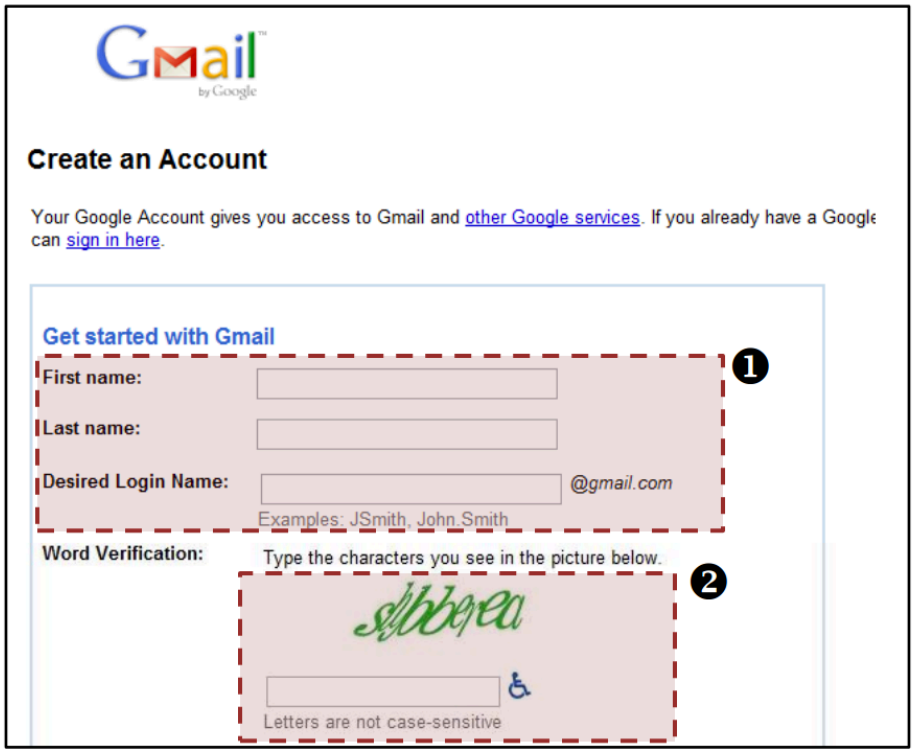
[Motoyama et al.]

Outsourcing jobs

- Freelancer.com: one of the largest outsourcing and oldest freelancing sites
  - Claims over 2 million employers and workers
  - User population covers 234 countries / regions
- How it works:
  - Buyer/employers post jobs
  - Workers bid on jobs
  - Buyers select workers

[Motoyama et al.]

- Scenario: Abuser wants to send spam via Web email
- Prerequisite: Bulk accounts on Gmail



❶

Gmail Fast Account Creator

Gmail Fast Account Creator is project number 359297
posted at Freelancer.com. Click here to post your own project.

❷

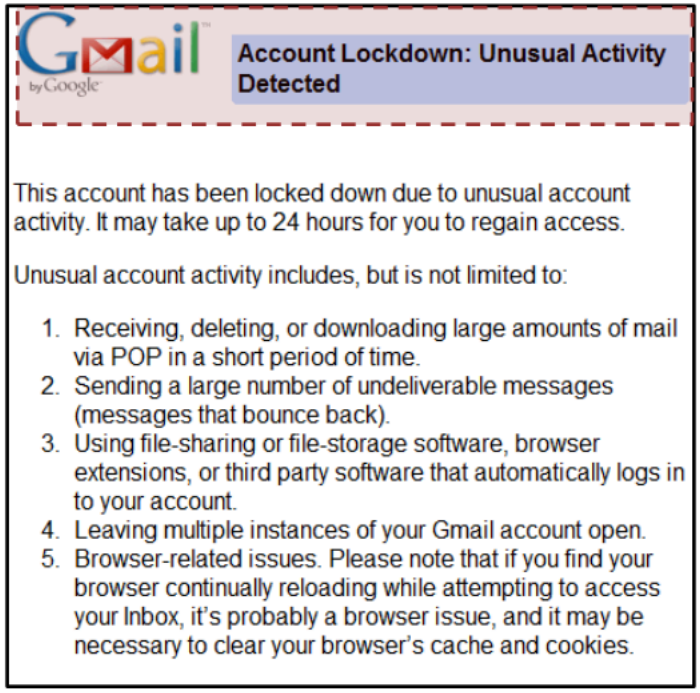
need gmail captcha codes entered

need gmail captcha codes entered is project number 452532
posted at Freelancer.com. Click here to post your own project.

"i need gmail captcha entry agent immediately. 1000's new captcha entrys per week

[Motoyama et al.]

- Problem: Google detects mass account creation
- Solution: Purchase IP proxy services



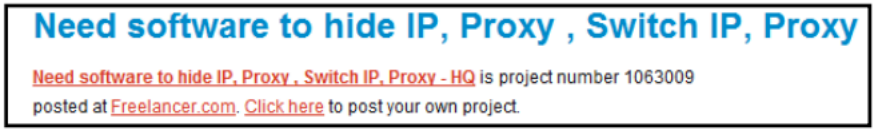
Gmail by Google

Account Lockdown: Unusual Activity Detected

This account has been locked down due to unusual account activity. It may take up to 24 hours for you to regain access.

Unusual account activity includes, but is not limited to:

1. Receiving, deleting, or downloading large amounts of mail via POP in a short period of time.
2. Sending a large number of undeliverable messages (messages that bounce back).
3. Using file-sharing or file-storage software, browser extensions, or third party software that automatically logs in to your account.
4. Leaving multiple instances of your Gmail account open.
5. Browser-related issues. Please note that if you find your browser continually reloading while attempting to access your Inbox, it's probably a browser issue, and it may be necessary to clear your browser's cache and cookies.

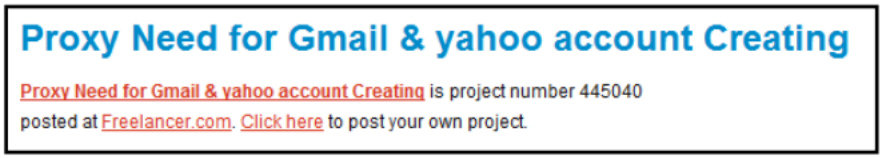


Need software to hide IP, Proxy , Switch IP, Proxy

Need software to hide IP, Proxy , Switch IP, Proxy - HQ is project number 1063009 posted at Freelancer.com. Click here to post your own project.

Proxy - We Need THOUSANDS of USA Anonymous I

Proxy - We Need THOUSANDS of USA Anonymous Proxies is project number 1098131 posted at Freelancer.com. Click here to post your own project.

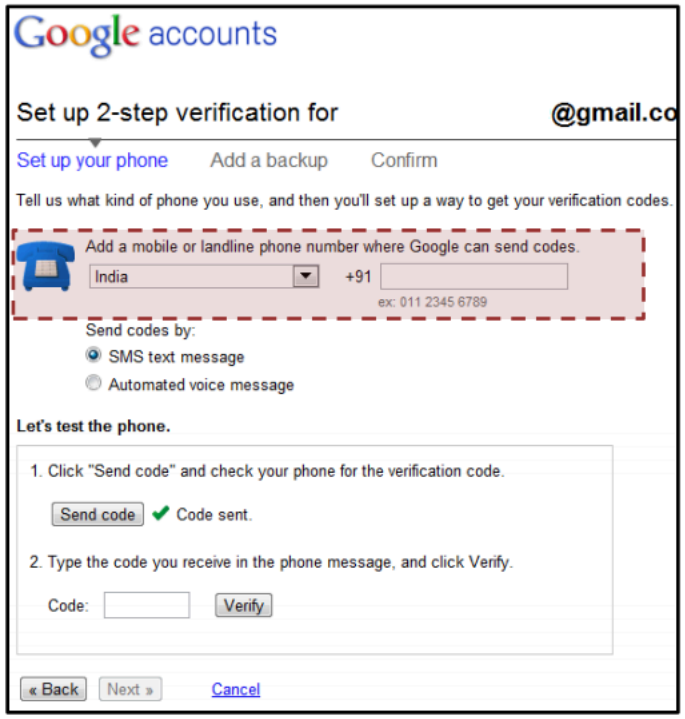


Proxy Need for Gmail & yahoo account Creating

Proxy Need for Gmail & yahoo account Creating is project number 445040 posted at Freelancer.com. Click here to post your own project.

[Motoyama et al.]

- Problem: Google implements phone verification
- Solution: Buy telephone numbers



Need U.S. Based Phone Numbers For PVA Verification

Need U.S. Based Phone Numbers For PVA Verification is project number 613869 posted at Freelancer.com. Click here to post your own project.

100 DID Forwarding Numbers for PVA Creation

100 DID Forwarding Numbers for PVA Creation is project number 484506 posted at Freelancer.com. Click here to post your own project.

1K Phone Activated Gmail Accounts Wanted

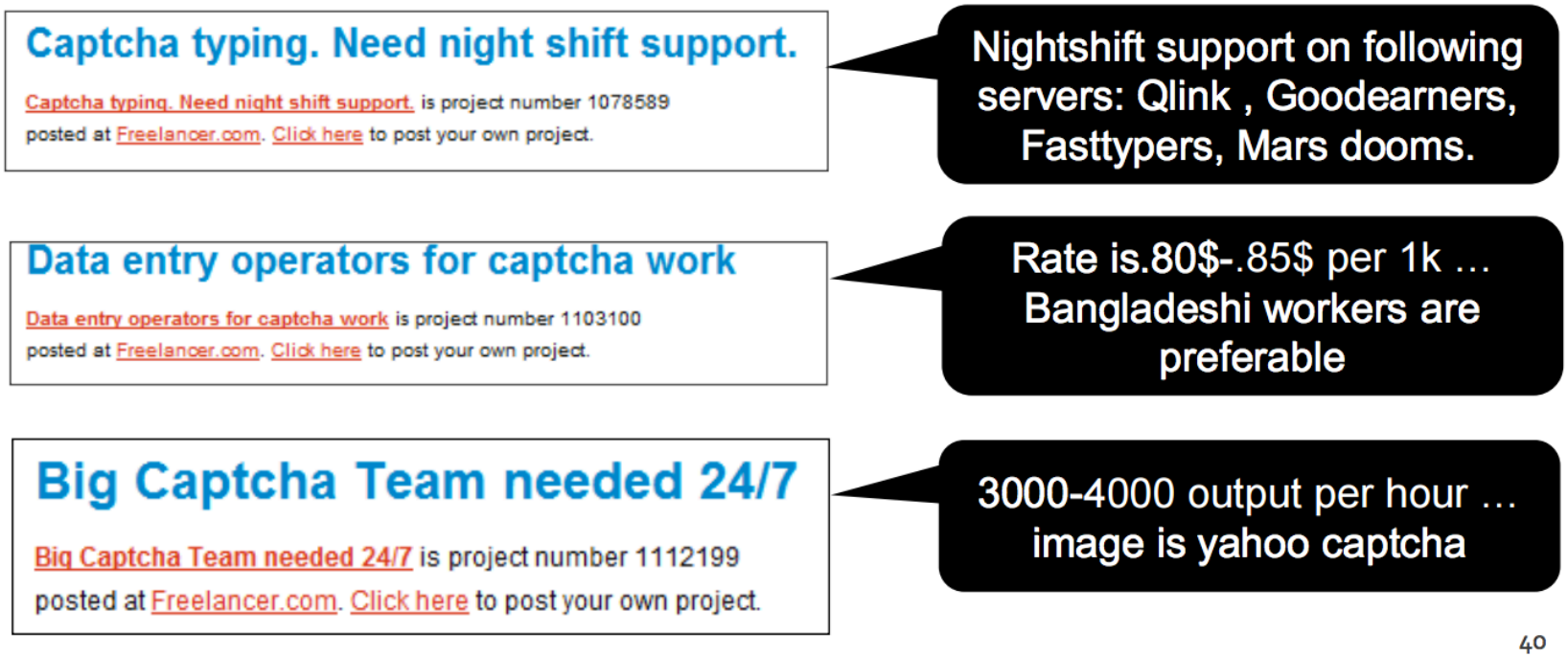
1K Phone Activated Gmail Accounts Wanted is project number 565733 posted at Freelancer.com. Click here to post your own project.

6

[Motoyama et al.]

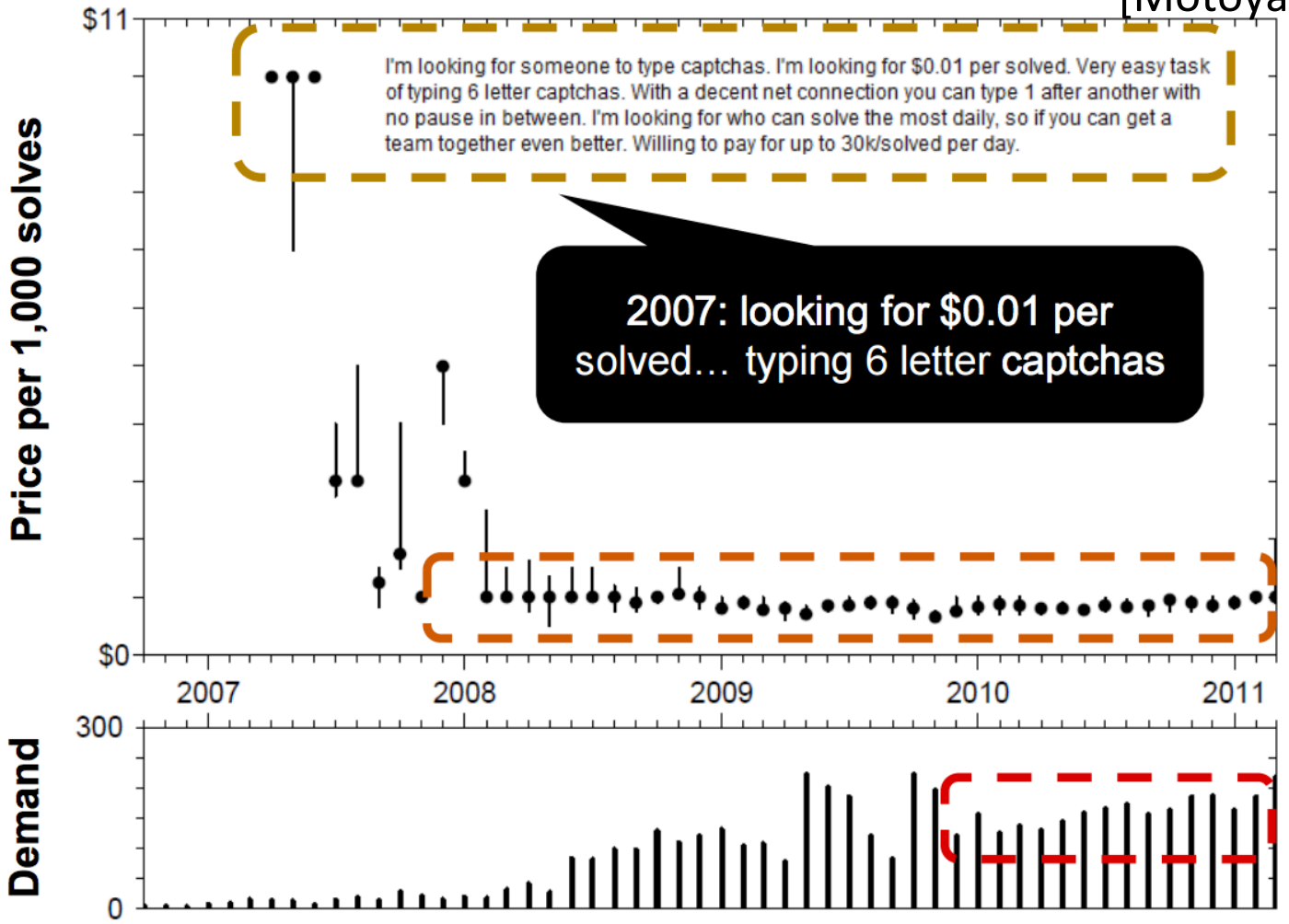
CAPTCHA Solving

- Overview: Using humans to solve CAPTCHAs
- Employers post daily ads on Freelancer.com:



40

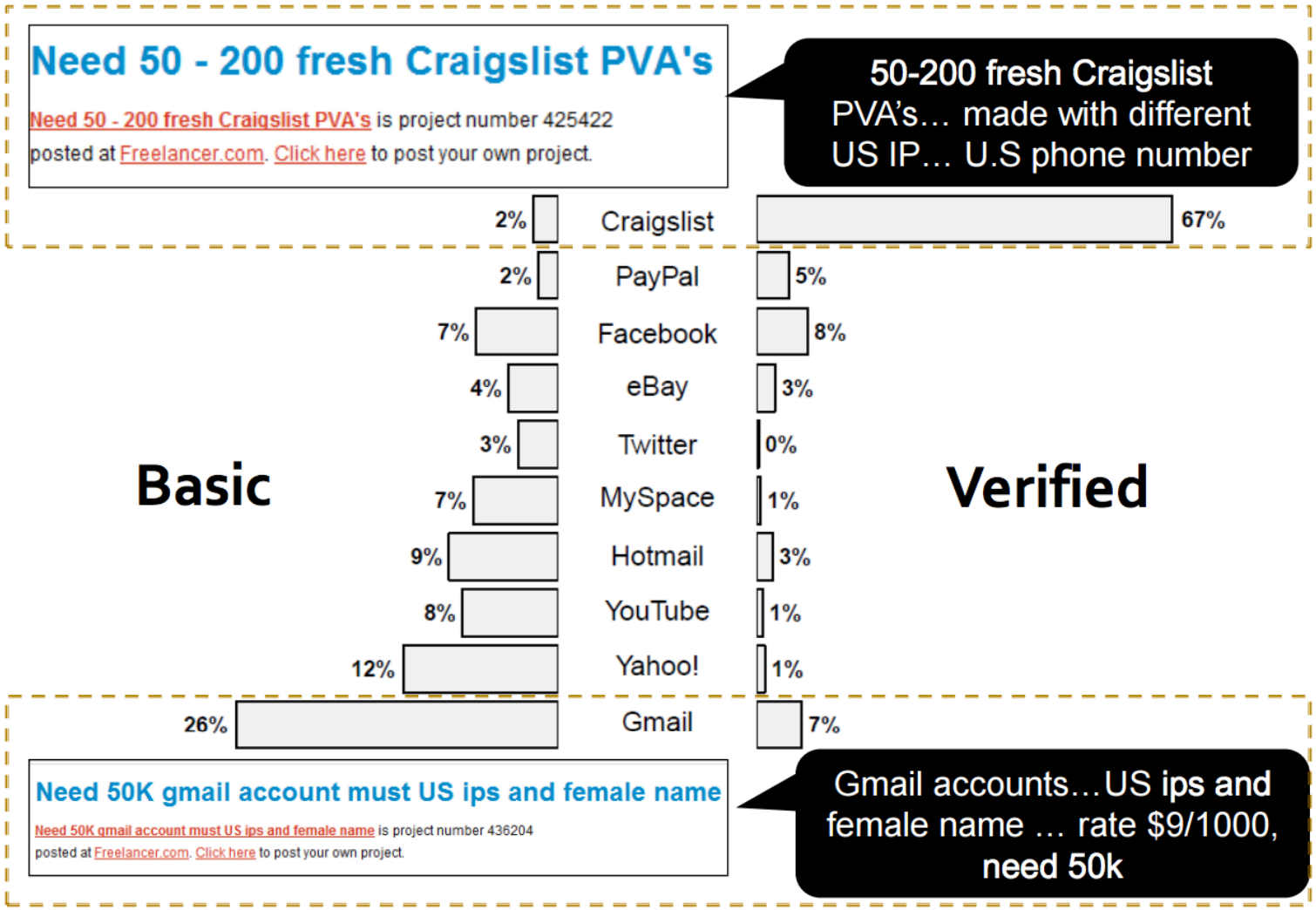
[Motoyama et al.]



- CAPTCHA solving began at nearly $10/1,000 solves
- Price stabilized to roughly $1/1,000 solves
- Demand has remained stable since 2010

[Motoyama et al.]

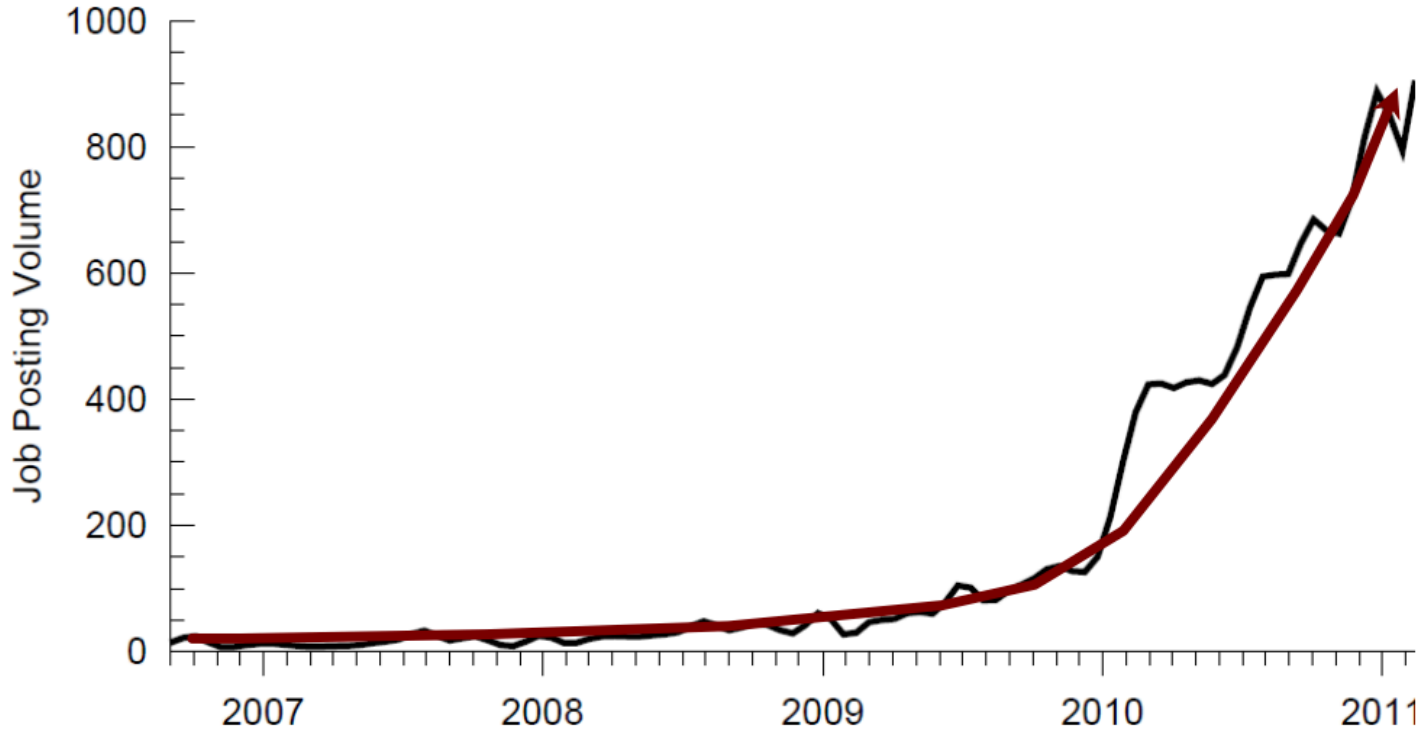
Example Jobs: Accounts



[Motoyama et al.]

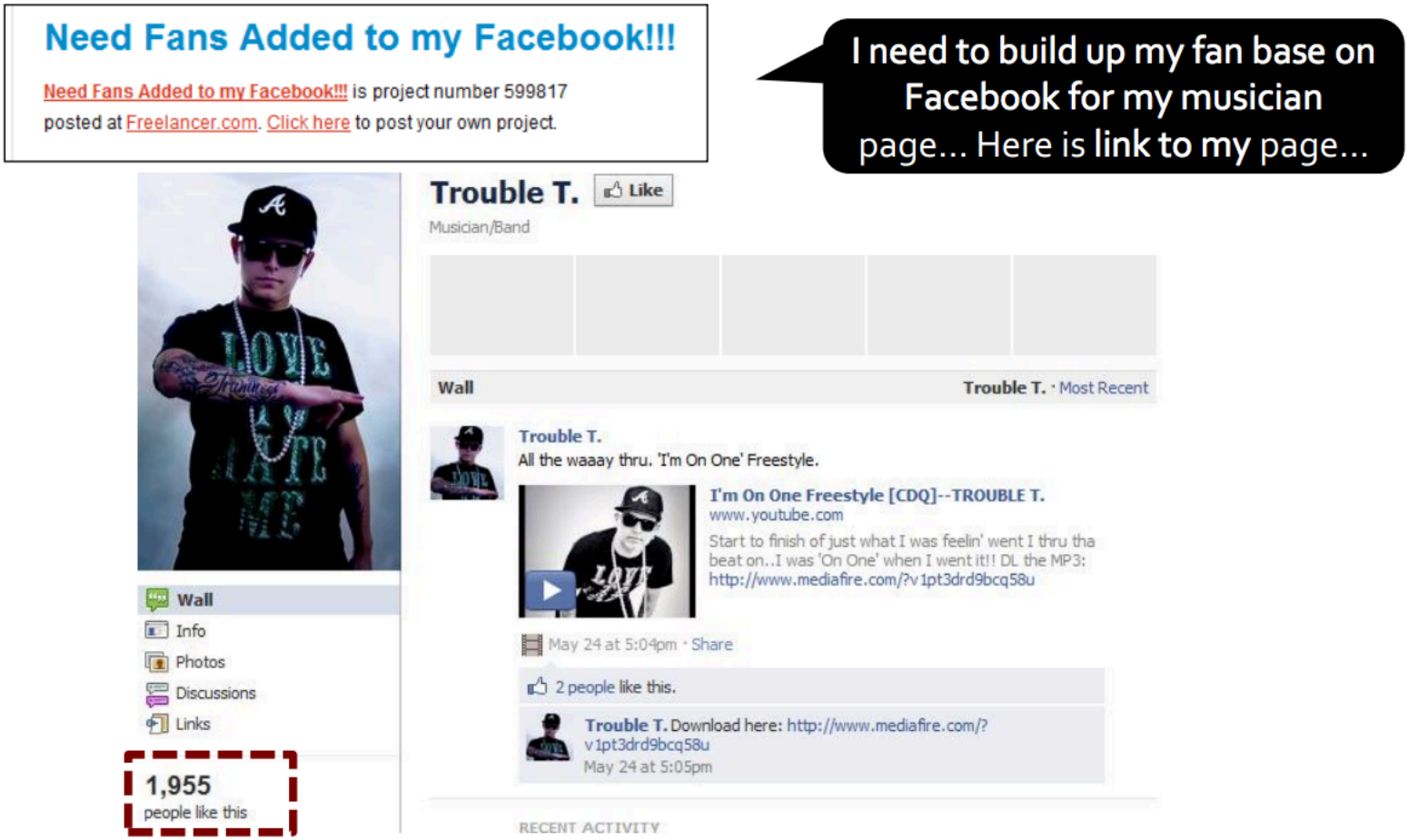
OSN Linking

- Buying friends, Facebook fans/lines for website pages, Twitter followers, YouTube subs, etc



[Motoyama et al.]

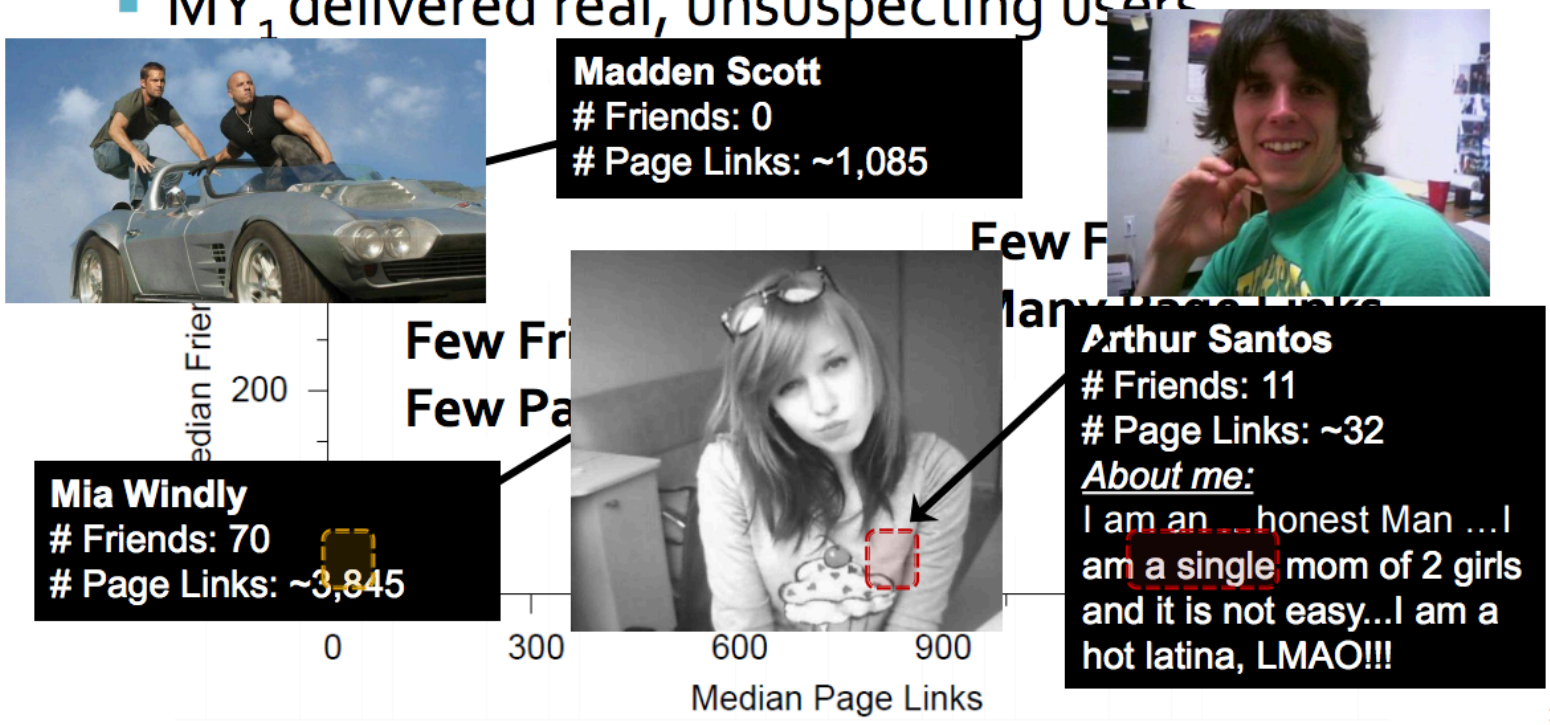
Example: Online Social Network Link



[Motoyama et al.]

User accounts

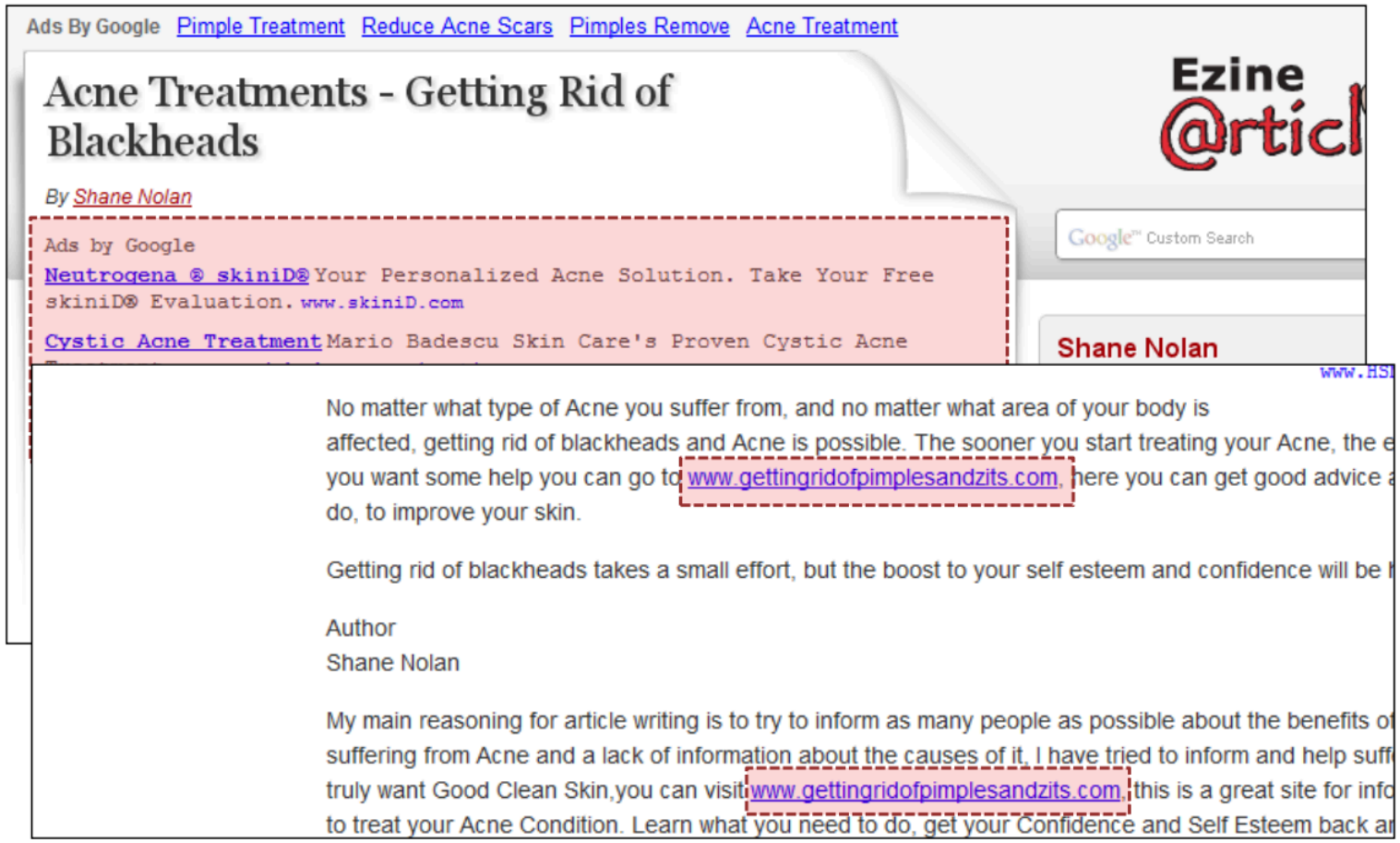
- Users are fake: few friends, substantial number of links to other websites
  - MY_1 delivered real, unsuspecting users



25

[Motoyama et al.]

Search Engine-Oriented Content



[Motoyama et al.]

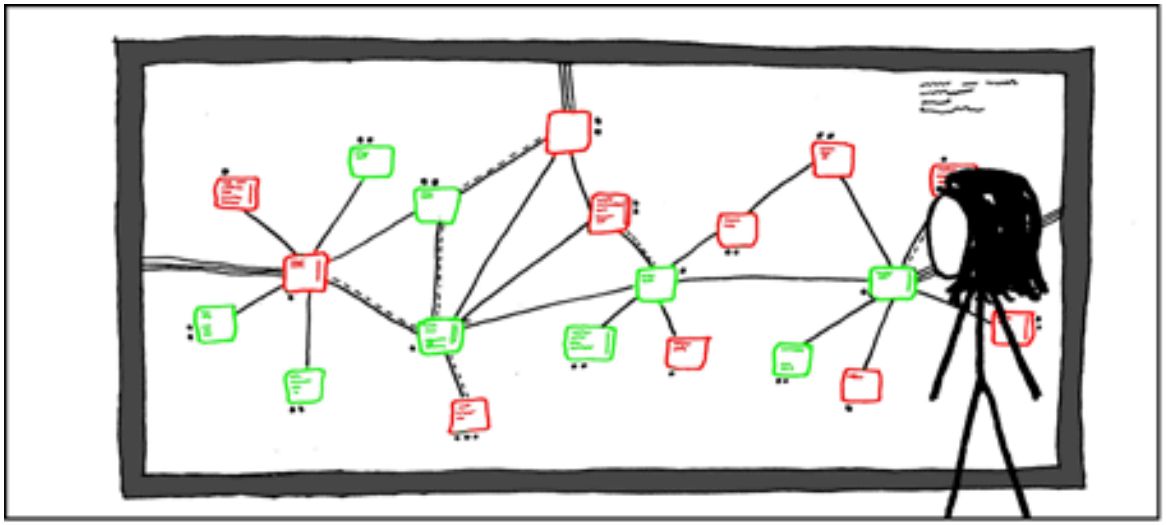
Freelance Abuse (USENIX 2011)

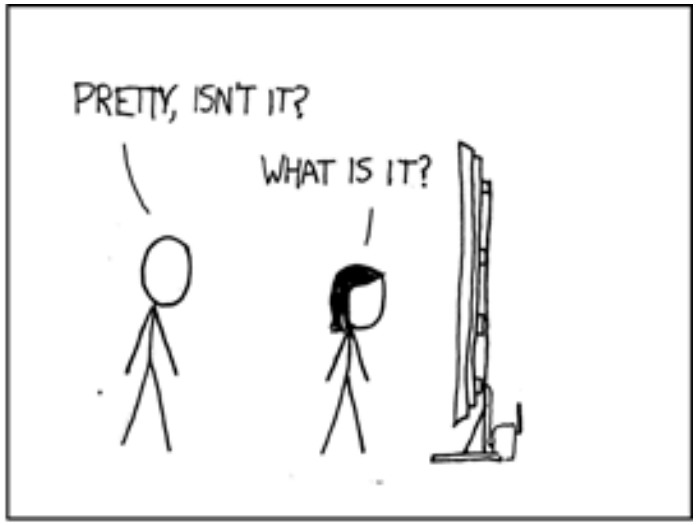
Category	Job Type	Description	Count	%
Legitimate [§A.1]	Web Design/Coding	Create, modify, or design a Web site	769	38.5
	Multimedia Related	Complete multimedia-related task (e.g., Flash)	265	13.2
	Private Jobs	Jobs designated for a particular worker	138	6.9
	Desktop/Mobile Applications	Create a desktop or mobile application	100	5.0
	Legitimate Miscellaneous	Miscellaneous jobs	177	8.8
Accounts [§A.2]	Account Registrations	Create accounts with no defined requirements	22	1.1
	Human CAPTCHA Solving	Requests for human CAPTCHA solving	19	0.9
	Verified Accounts	Create verified accounts (e.g. phone)	14	0.7
SEO [§A.3]	SEO Content Generation	Requests for SEO content (e.g., articles, blogs)	195	9.8
	Link Building (Grey Hat)	Get backlinks using grey hat methods	53	2.6
	Link Building (White Hat)	Get backlinks using no grey/black hat methods	20	1.0
	SEO Miscellaneous	Nonspecific SEO-related job postings	61	3.0
Spamming [§A.4]	Ad Posting	Post content for human consumption	25	1.2
	Bulk Mailing	Send bulk emails	8	0.4
OSN Linking [§A.5]	Create Social Networking Links	Get friends/subscribers/fans/followers/etc.	33	1.7
Misc [§A.6]	Abuse Tools	Tools used for abuse (e.g., CAPTCHA OCR)	41	2.1
	Clicks/CPA/Leads/Signups	Get clicks, emails, zip codes, signups, etc.	32	1.6
	Manual Data Extraction	Manually visit websites and scrape content	21	1.1
	Gather Email/Contact Lists	Research contact details for targeted people	17	0.9
	Academic Fraud	Write essays, code homework assignments, etc.	10	0.5
	Reviews/Astroturfing	Create positive reviews	1	0.1
	Other Malicious	Miscellaneous jobs with malicious intentions	35	1.8

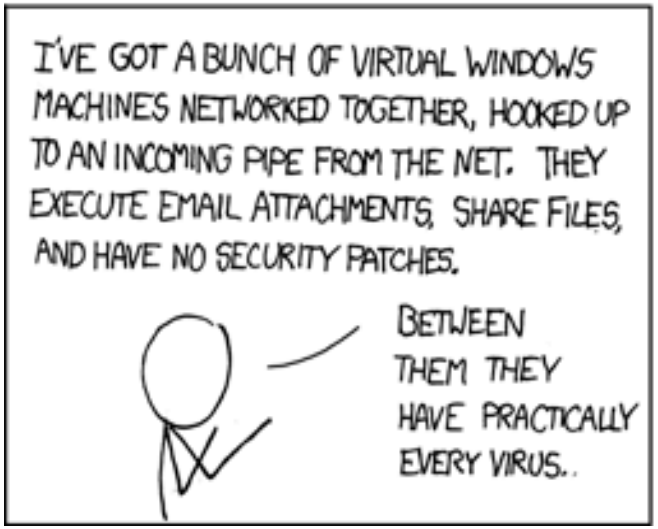
[Motoyama et al.]

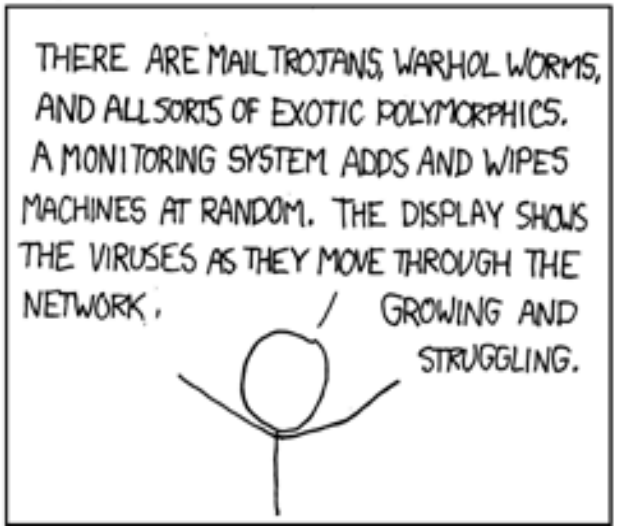
Summary

- Attackers outsource abuse jobs
  - ~30% of Freelancer.com jobs abusive
  - Jobs spanned range of categories from spamming to account registration
- Quality of product is highly variable
- Large, cheap labor pool changes threat model
  - Automation is not the only way
  - Largely removes difficulty in executing abuse task
- Outsourced workforce enables new attacks




PRETTY, ISN'T IT?
WHAT IS IT?


I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS.


THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK.
GROWING AND STRUGGLING.


YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!