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”]

[Map of the world showing the spread of the Sapphire/Slammer Worm on January 25, 2003.]
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
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)

- **Attacker**
  - Master machines
    - Zombie machines
      - Victim
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 (Completely Automated Public Turing test to tell Computers and Humans Apart)

• 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
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

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

![Gmail Fast Account Creator](image)

1. **Gmail Fast Account Creator**
   - Gmail Fast Account Creator is project number 359297
   - posted at [Freelancer.com](http://Freelancer.com). Click here to post your own project.

2. **need gmail captcha codes entered**
   - need gmail captcha codes entered is project number 452532
   - posted at [Freelancer.com](http://Freelancer.com). Click here to post your own project.

"i need gmail captcha entry agent immediately. 1000's new captcha entries per week"
- Problem: Google detects mass account creation
- Solution: Purchase IP proxy services

![Google Account Lockdown: Unusual Activity Detected](image1)

**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](http://Freelancer.com), [Click here](http://Click here) to post your own project.

**Proxy - We Need THOUSANDS of USA Anonymous IP**
Proxy - We Need THOUSANDS of USA Anonymous Proxies is project number 1098131
posted at [Freelancer.com](http://Freelancer.com), [Click here](http://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](http://Freelancer.com), [Click here](http://Click here) to post your own project.
Problem: Google implements phone verification
Solution: Buy telephone numbers
CAPTCHA Solving

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

  - Captcha typing. Need night shift support.
    - Nightshift support on following servers: Qlink, Goodearners, Fasttypers, Mars dooms.
  - Data entry operators for captcha work
    - Rate is $0.80 - $0.85 per 1k … Bangladeshi workers are preferable
  - Big Captcha Team needed 24/7
    - 3000-4000 output per hour … image is yahoo captcha
2007: looking for $0.01 per solved... typing 6 letter captchas

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

Need 50 - 200 fresh Craigslist PVA's

Need 50 - 200 fresh Craigslist PVA's is project number 425422
posted at [Freelancer.com](https://www.freelancer.com). Click here to post your own project.

- Craigslist: 2% (67%)
- PayPal: 2%
- Facebook: 7%
- eBay: 4%
- Twitter: 3%
- MySpace: 7%
- Hotmail: 9%
- YouTube: 8%
- Yahoo!: 12%
- Gmail: 26%

50-200 fresh Craigslist PVA's... made with different US IP... U.S phone number

Basic

Verified

Gmail accounts... US ips and female name ... rate $9/1000, need 50k

Need 50K gmail account must US ips and female name

Need 50K gmail account must US ips and female name is project number 436924
posted at [Freelancer.com](https://www.freelancer.com). Click here to post your own project.
OSN Linking

• Buying friends, Facebook fans/lines for website pages, Twitter followers, YouTube subs, etc
Example: Online Social Network Link

Need Fans Added to my Facebook!!!

I need to build up my fan base on Facebook for my musician page... Here is link to my page...

[Link to Facebook page]
User accounts

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

- Example:
  - Madden Scott
    - # Friends: 0
    - # Page Links: ~1,085
  - Mia Windly
    - # Friends: 70
    - # Page Links: ~3,845
  - Arthur Santos
    - # Friends: 11
    - # Page Links: ~32
    - About me:
      I am an... honest Man ...I am a single mom of 2 girls and it is not easy...I am a hot latina, LMAO!!!
Search Engine-Oriented Content

Acne Treatments - Getting Rid of Blackheads

By Shane Nolan

No matter what type of Acne you suffer from, and no matter what area of your body is affected, getting rid of blackheads and Acne is possible. The sooner you start treating your Acne, the easier it will be to get rid of blackheads. Here are some steps you can take:

1. Wash your face with a mild cleanser twice a day.
2. Avoid touching or picking at your face.
3. Use a comedone extractor to remove blackheads.
4. Apply a treatment product that contains benzoyl peroxide or salicylic acid.

[Insert image with article snippet]

www.gettingridofpimplesandzits.com

My main reason for article writing is to try to inform as many people as possible about the benefits of using a personalized acne treatment and the importance of taking care of your skin. Good Clean Skin, you can visit www.gettingridofpimplesandzits.com, this is a great site for information on how to treat your Acne Condition. Learn what you need to do, get your Confidence and Self Esteem back and keep your face looking healthy.

www.gettingridofpimplesandzits.com
## Freelance Abuse (USENIX 2011)

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