This time

On top of the stack

Application-layer security

Peering into

Underground Economies
Final exam

Wednesday May 18
10:30 AM – 12:30 PM
HERE (CSIC 2117)

• Cumulative
  • Software security
  • Crypto
  • Networking
Teaching evaluations

Please set aside some time this week to do them!
On top of the stack
Application-layer security
Application layer

• Familiar faces:
  • HTTP (web)
  • SMTP (mail)
  • Skype
  • Bittorrent
  • Gaming ..... 

• All of these choose explicitly from the layer beneath them (UDP vs TCP)
  • TCP when you must have reliable, in-order delivery
    - Web, mail, BitTorrent
  • UDP when you prefer timeliness over reliability
    - Gaming, Skype
In what layer should security go?

• Fundamental principle: the **end-to-end principle** (applies to reliability in general)

• If there is a function that can be implemented correctly and completely only at the end hosts, then put it there, not in the network.
  • Exception: the network can be used as a performance enhancement

• How can TCP know what it means to secure your application?
  • Does it just need encryption? Key sharing? Obfuscated timing? ….?
Example of the SMTP Procedure

This SMTP example shows mail sent by Smith at host Alpha.ARPA, to Jones, Green, and Brown at host Beta.ARPA. Here we assume that host Alpha contacts host Beta directly.

S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK

S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK

S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here

S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK

S: DATA
R: 354 Start mail input; end with <CRLF><CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF><CRLF>
R: 250 OK

The mail has now been accepted for Jones and Brown. Green did not have a mailbox at host Beta.

Example 1
Example: SMTP (RFC 821)

Example of the SMTP Procedure

This SMTP example shows mail sent by Smith at host Alpha.ARPA, to Jones, Green, and Brown at host Beta.ARPA. Here we assume that host Alpha contacts host Beta directly.

S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK

S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK

S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here

S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK

S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK

The mail has now been accepted for Jones and Brown. Green did not have a mailbox at host Beta.

Example 1

These are all just packets and you can construct whatever packets you want.
In what layer should security go?

• Need to understand what properties you get from each layer

• If you require a property that cannot be guaranteed by the underlying layers, then you have to add it to the “end”

• Email: how would you fix this?
  • You want authentic communication
  • Can you build it out of an unauthenticated channel?
Protecting your network

• How do you harden a set of systems against an external attack?

• Challenge: attack surface
  • The more network services your machines run, the greater the risk

• One approach: turn off unnecessary network services
  • But you have to know all the services
  • And sometimes trusted remote users still require access

• Challenge: scaling to 100s or 1000s of systems
Scalable solution to management complexity

• Reduce risk by blocking from *within the network* any outsiders from having unwanted access

• Interpose a **firewall** as a reference monitor on traffic
Scalable solution to management complexity

• Reduce risk by blocking from *within the network* any outsiders from having unwanted access

• Interpose a **firewall** as a reference monitor on traffic

What do we know about reference monitors?
Scalable solution to management complexity

• Reduce risk by blocking from *within the network* any outsiders from having unwanted access

• Interpose a firewall as a reference monitor on traffic

  What do we know about reference monitors?

  **You must ensure complete mediation**

• Firewalls can typically cover thousands of hosts
  • Need to find a chokepoint in your network
  • Where do chokepoints normally exist?
Security policies

• Network security policy:
  • what hosts are allowed to talk to what other hosts,
  • and who is allowed to access what service?

• Distinguish between inbound and outbound connections
  • Outbound: internal users accessing external services
  • Inbound: external users attempting to connect to services on internal machines

• Why distinguish inbound/outbound?
  • Because it fits with a common threat model
Security policies

• Firewalls permit a conceptually simple **access control policy**
  • Permit *inside* users to connect to any service
  • Restrict *external* users:

• External users:
  • Permit connections to services that are meant to be externally visible
  • Deny connections services that are not meant to be externally visible
Expressing firewall policies

• Typically represented by a prioritized list of match/action pairs.
  • Perform the action corresponding to the highest-priority rule that matches

• Example actions
  • Allow the traffic to flow
  • Drop the traffic
  • Also possibly rate-limit the traffic

• Matching rules
  • **Traditional firewall**: operates over header data (src-IP, src-port, dst-IP, dst-port, protocol, TCP flags)
  • **Application-layer firewall**: also include application-layer data (perform “deep packet inspection” that looks at the payloads, not just the headers)
Great firewall of China

• Uses many of the same techniques in firewalls
  • What is the difference?

• Also uses “application-layer” firewalls
  • Inspects payloads
    - E.g., requested domain names in DNS queries
  • And can inject application-layer responses to censor
    - E.g., can reply to wikipedia.org DNS query with a lemon IP
Getting around the Great Firewall of China
Getting around the Great Firewall of China

• If the src or dst is in the country, then all traffic must go through the firewall
  • Common approach: confidentiality
    - Countermeasure: block Tor traffic (or other encrypted traffic) to all but a specific set of hosts (for businesses who use VPNs)
  • New approach: protocol obfuscation
    - Make a protocol the country disallows (e.g., Tor) look like another that the country is ok with (e.g., Skype)
  • New approach: decoy routing
    - Make it look like you are talking to destination D but a router on the path redirects you to your true destination D'.
Getting around the Great Firewall of China

• If the src or dst is in the country, then all traffic *must* go through the firewall
  • Common approach: *confidentiality*
    - Countermeasure: block Tor traffic (or other encrypted traffic) to all but a specific set of hosts (for businesses who use VPNs)
  • New approach: *protocol obfuscation*
    - Make a protocol the country disallows (e.g., Tor) look like another that the country is ok with (e.g., Skype)
  • New approach: *decoy routing*
    - Make it look like you are talking to destination D but a router on the path redirects you to your true destination D'.

Avoiding censorship from a “routing-capable adversary” is one of the most challenging open problems
Getting around the Great Firewall of China

• Even if *neither* source nor destination are in China, they can *still be censored* if their traffic goes *through* China
  • This censorship-in-transit is sometimes called “collateral damage”
  • Similar things elsewhere: “boomerang routing” leads, e.g., two hosts in Brazil to have their traffic routed through the US.
  • There is general concern as to what intermediate countries are doing with our traffic

• New approach: “Alibi routing”
  • “I want to communicate with destination D but I want proof that my packets avoided these regions of the world…”
Peering into Underground Economies
Underground economies

• Economics drives both the attacks and the defenses

• What is for sale? Who sells it? How?
  • Defenders: Antivirus vendors, firewall vendors, etc.
  • What about the attackers?

• The idea is that we may be able to stem attacks if we can understand
  • the incentives
  • the choke points (might there be one bank we could shut down to cease spam?)
• **Who buys**: Attackers, spies (and the companies who wrote the software) want to know about them.

• **Through whom**: anonymous middlemen (e.g. Grusq) who match vulnerability finders up with buyers. Take commission (15% typical).

• **Payment**: Made in installments (cease payment when zero-day over).
• **Who buys**: Attackers, spies (and the companies who wrote the software) want to know about them

• **Through whom**: anonymous middlemen (e.g. Grusq) who match vulnerability finders up with buyers. Take commission (15% typical).

• **Payment**: Made in installments (cease payment when zero-day over)

Google offers a max of $3133.70 for information about flaws in their tech.
• **Who buys**: Attackers, spies (and the companies who wrote the software) want to know about them.

• **Through whom**: anonymous middlemen (e.g. Grusq) who match vulnerability finders up with buyers. Take commission (15% typical).

• **Payment**: Made in installments (cease payment when zero-day over)

Google offers a max of $3133.70 for information about flaws in their tech

<table>
<thead>
<tr>
<th>Software</th>
<th>Reward Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADOBE READER</td>
<td>$5,000–$30,000</td>
</tr>
<tr>
<td>MAC OSX</td>
<td>$20,000–$50,000</td>
</tr>
<tr>
<td>ANDROID</td>
<td>$30,000–$60,000</td>
</tr>
<tr>
<td>FLASH OR JAVA BROWSER PLUG-INS</td>
<td>$40,000–$100,000</td>
</tr>
<tr>
<td>MICROSOFT WORD</td>
<td>$50,000–$100,000</td>
</tr>
<tr>
<td>WINDOWS</td>
<td>$60,000–$120,000</td>
</tr>
<tr>
<td>FIREFOX OR SAFARI</td>
<td>$60,000–$150,000</td>
</tr>
<tr>
<td>CHROME OR INTERNET Explorer</td>
<td>$80,000–$200,000</td>
</tr>
<tr>
<td>IOS</td>
<td>$100,000–$250,000</td>
</tr>
</tbody>
</table>

“Shopping for zero-days” Forbes 2012
Spam

• Unsolicited, annoying email (or posts on blogs, social networks, etc.) that seeks to
  • Sell products
  • Get users to install malicious software

• Typical defenses
  • Look for key words in the messages
  • Block certain senders (SpamHaus blacklist of IP addrs)

• But what is the economics behind it all?
  • How do they send out so much email?
  • Are they selling real things? How?
Sending spam

• Tons of email to send, and easy to block a single IP address from sending

• Need lots of IP addresses
  • But since SMTP (email) uses TCP, we need to actually be able to operate those IP addresses

• Buy lots of computers? (expensive)
Sending spam

• Tons of email to send, and easy to block a single IP address from sending

• Need lots of IP addresses
  • But since SMTP (email) uses TCP, we need to actually be able to operate those IP addresses

• Buy lots of computers? (expensive)

Compromise lots of computers!
**Botnet**

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)

- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!

- Upon infection, a new bot “phones home” to *rendezvous* with botnet “command-and-control” (C&C)

- Botmaster uses C&C to push out commands and updates
Botnet

• Collection of compromised machines (bots) under unified control of an attacker (botmaster)

• Method of compromise decoupled from method of control
  • Launch a worm/virus, etc.: remember, payload is orthogonal!

• Upon infection, a new bot “phones home” to rendezvous with botnet “command-and-control” (C&C)

• Botmaster uses C&C to push out commands and updates
Botnet

• Collection of compromised machines (bots) under unified control of an attacker (botmaster)

• Method of compromise decoupled from method of control
  • Launch a worm/virus, etc.: remember, payload is orthogonal!

• Upon infection, a new bot “phones home” to rendezvous with botnet “command-and-control” (C&C)

• Botmaster uses C&C to push out commands and updates
Botnet

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)

- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!

- Upon infection, a new bot “phones home” to rendezvous with botnet “command-and-control” (C&C)

- Botmaster uses C&C to push out commands and updates
Botnet

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)

- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!

- Upon infection, a new bot “phones home” to rendezvous with botnet “command-and-control” (C&C)

- Botmaster uses C&C to push out commands and updates

Topology can be star (like this), hierarchical, peer-to-peer…
Supporting clicks

• Ideally a user will click on an embedded URL

• Result is more complex than just going to a web server
  • Defensive measures: URL and domain blacklisting & takedown notices by ISPs

• Confuse defenses (esp. blacklisting) with moving targets:
  • Redirection sites (legit-looking URL, like a URL shortener, or just manage DNS yourself and create throwaway domains that redirect to a more permanent domain)
  • Bulk domains: purchased from a reseller or as part of an affiliate program (more later)

• But web servers are static, so how do we keep them from being shut down due to blacklisting and takedown notices?
Spambot

Botnet used for sending spam

TCP

HTTP

Proxy bots

Workers
Spambot

Botnet used for sending spam
Spambot

Botnet used for sending spam

Web server
Web server
Web server
Name server

TCP
HTTP

Proxy bots
Workers

“Bulletproof hosting” services
Bulletproof hosting sites

• Services / specific hosts are often blocked by appealing to their ISPs ("please block this user..")

• Bulletproof hosting services will refuse to block you (for a price)

• Many have been taken down
  • Often linked to criminal organizations

• Storm botnet: Controller likely run by Russian Business Network
  • Used Atrivo as their bulletproof hosting service
Why multiple levels of indirection

• Many workers send email

• User clicks: gets sent to a proxy bot, who redirects to a web server

• Why proxies?
  • To subvert defenses that block IP addresses
  • Keep the IP address for a given host (buydrugs.ru) moving

• “Fast flux” network
  • Short-lived TTLs in DNS responses (hostname to IP address mapping changes quickly)
  • Web proxies to a set of fixed web servers
Quick botnet aside...
Monetizing botnets

• **General malware monetization** approaches apply:
  • Keyloggers (steal financial, email, social network, etc. accounts)
  • Ransomware
  • Transaction generators
    - Watch user’s surfing
    - Wait to log into banking site and inject extra money, then alter web server replies to mask change in user balance
    - Or wait until the user clicks and inject your own, too.
Monetizing botnets

• Additionally, botnets give you massive scale
  • DDoS
  • Click fraud
  • Scam infrastructure
    • Hosting web pages (e.g., for phishing)
    • Redirection to evade blacklisting/takedown notices
  • Spam
Monetizing botnets

• Additionally, botnets give you massive scale
  • DDoS
  • Click fraud
  • Scam infrastructure
    - Hosting web pages (e.g., for phishing)
    - Redirection to evade blacklisting/takedown notices
  • Spam

None of these cause serious pain for the infected user!

Users have little incentive to prevent these
Advertising your botnet

How do you advertise the capabilities of your amazing botnet?
Advertising your botnet

How do you advertise the capabilities of your amazing botnet?

Some DNS root servers advertise query volume
“see how much attack traffic we can fend off!”
Advertising your botnet

How do you advertise the capabilities of your amazing botnet?

Some DNS root servers advertise query volume “see how much attack traffic we can fend off!”
Advertising your botnet

How do you advertise the capabilities of your amazing botnet?

Some DNS root servers advertise query volume “see how much attack traffic we can fend off!”

“Look for the surge 4 days from now”
The importance of botnets

• Botnets represent the “great modern threat” of the Internet

• Why not worms?
The importance of botnets

• Botnets represent the “great modern threat” of the Internet

• Why not worms?
  - Greater control over botnets
  - Less emergent
  - Quieter
  - Flexible
Taking down botnets
Taking down botnets

• Approach #1: **prevent** the initial bot infection
  • Infection is decoupled from bot’s participation in the botnet, so this is equivalent to preventing malware infections in general - *hard*

• Approach #2: **Take down** the C&C master server

• Botmaster counter-measures?
Taking down botnets

• Approach #1: prevent the initial bot infection
  • Infection is decoupled from bot’s participation in the botnet, so this is equivalent to preventing malware infections in general - hard

• Approach #2: Take down the C&C master server

• Botmaster counter-measures?
  - Move the C&C around: each day (e.g.) bots generate a large list of possible domain names.
  - Try a random subset looking for C&C server.
  - Server signs its replies
Taking down botnets

• Approach #1: **prevent** the initial bot infection
  • Infection is decoupled from bot’s participation in the botnet, so this is equivalent to preventing malware infections in general - *hard*

• Approach #2: **Take down** the C&C master server

• Botmaster counter-measures?
  - Move the C&C around: each day (e.g.) bots generate a large list of possible domain names.
  - Try a random subset looking for C&C server.
  - Server signs its replies

**Counter-counter measure?**
...back to spam
Affiliate programs

Markets drive efficiency and specialization: some specialize in botnets, others in spam

• You can join an affiliate program!
  • You send out emails and get a commission (30–50%)  

• Affiliate program provides:
  • Storefront templates, shopping cart management
  • Analytics support
  • Advertising materials
  • Central web service interface for affiliates to track conversions and to register for payouts
  • Domains bought in bulk
  • …
Realization: Getting paid

Customer ➔ Issuing bank ➔ Card association network (e.g., Visa, MasterCard) ➔ Acquiring bank ➔ Payment processor ➔ Merchant

Facilitates payment
Realization: Shipping goods

- Business-to-business websites will make connections across many different goods
  - Alibaba, EC-Plaza, ECTrade, ...

- Commonly offer “drop shipping”
  - The spambot operator does not need to purchase any warehouse/storage
Figure 1: Infrastructure involved in a single URL’s value chain, including advertisement, click support and realization steps.
1. Spam delivered

Figure 1: Infrastructure involved in a single URL’s value chain, including advertisement, click support and realization steps.
1. Spam delivered
2. User clicks
1. Spam delivered
2. User clicks
3. Domain registered by reg.ru
1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`
4. Nameserver hosted in China
1. Spam delivered
2. User clicks
3. Domain registered by reg.ru
4. Nameserver hosted in China
5. Renders storefront
1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`
4. Nameserver hosted in China
5. Renders storefront
6. Analytics updated at affiliate

Figure 1: Infrastructure involved in a single URL’s value chain, including advertisement, click support and realization steps.
1. Spam delivered
2. User clicks
3. Domain registered by \textit{reg.ru}
4. Nameserver hosted in China
5. Renders storefront
6. Analytics updated at affiliate
7. User makes payment; acquiring bank in Azerbaijan
1. Spam delivered
2. User clicks
3. Domain registered by reg.ru
4. Nameserver hosted in China
5. Renders storefront
6. Analytics updated at affiliate
7. User makes payment; acquiring bank in Azerbaijan
8. Supplier in Chennai, India delivers 10 days later
Analyzing spam "click trajectories"

Measurement study out of UCSD
Who/what gets sold

• Three most common products sold:
  • Pharmaceuticals (vast majority)
  • Replica luxury goods
  • Counterfeit software

• Run by relatively few affiliate programs

<table>
<thead>
<tr>
<th>Stage</th>
<th>Pharmacy</th>
<th>Software</th>
<th>Replicas</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>URLs</td>
<td>346,993,046</td>
<td>3,071,828</td>
<td>15,330,404</td>
<td>365,395,278</td>
</tr>
<tr>
<td>Domains</td>
<td>54,220</td>
<td>7,252</td>
<td>7,530</td>
<td>69,002</td>
</tr>
<tr>
<td>Web clusters</td>
<td>968</td>
<td>51</td>
<td>20</td>
<td>1,039</td>
</tr>
<tr>
<td>Programs</td>
<td>30</td>
<td>5</td>
<td>10</td>
<td>45</td>
</tr>
</tbody>
</table>

Table III: Breakdown of clustering and tagging results.
Few affiliate programs constitute the majority

<table>
<thead>
<tr>
<th>Affiliate Program</th>
<th>Distinct Domains</th>
<th>Received URLs</th>
<th>Feed Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxPrm</td>
<td>10,585</td>
<td>160,521,810</td>
<td>24.92%</td>
</tr>
<tr>
<td>Mailn</td>
<td>14,444</td>
<td>69,961,207</td>
<td>23.49%</td>
</tr>
<tr>
<td>PhEx</td>
<td>14,381</td>
<td>69,959,629</td>
<td>23.48%</td>
</tr>
<tr>
<td>EDEEx</td>
<td>63</td>
<td>1,578</td>
<td>0.01%</td>
</tr>
<tr>
<td>ZCashPh</td>
<td>6,976</td>
<td>42,282,943</td>
<td>14.54%</td>
</tr>
<tr>
<td>DrMax</td>
<td>5,641</td>
<td>32,184,860</td>
<td>10.95%</td>
</tr>
<tr>
<td>Grow</td>
<td>382</td>
<td>5,210,668</td>
<td>1.68%</td>
</tr>
<tr>
<td>USHC</td>
<td>167</td>
<td>3,196,538</td>
<td>1.31%</td>
</tr>
<tr>
<td>MaxGm</td>
<td>672</td>
<td>1,144,703</td>
<td>0.41%</td>
</tr>
<tr>
<td>VgREX</td>
<td>39</td>
<td>426,873</td>
<td>0.14%</td>
</tr>
<tr>
<td>Stud</td>
<td>42</td>
<td>68,907</td>
<td>0.03%</td>
</tr>
<tr>
<td>ManXt</td>
<td>33</td>
<td>50,394</td>
<td>0.02%</td>
</tr>
<tr>
<td>GlvMd</td>
<td>2,933</td>
<td>28,313,136</td>
<td>10.32%</td>
</tr>
<tr>
<td>OLPh</td>
<td>2,894</td>
<td>17,226,271</td>
<td>5.16%</td>
</tr>
<tr>
<td>Eva</td>
<td>11,281</td>
<td>12,795,646</td>
<td>8.7%</td>
</tr>
<tr>
<td>WldPh</td>
<td>691</td>
<td>10,412,850</td>
<td>3.55%</td>
</tr>
</tbody>
</table>
What gets sold

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Item</th>
<th>Origin</th>
<th>Affiliate Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aracoma Drug</td>
<td>Orange bottle of tablets (pharma)</td>
<td>WV, USA</td>
<td>ClFr</td>
</tr>
<tr>
<td>Combitic Global Caplet Pvt. Ltd.</td>
<td>Blister-packed tablets (pharma)</td>
<td>Delhi, India</td>
<td>GlvMd</td>
</tr>
<tr>
<td>M.K. Choudhary</td>
<td>Blister-packed tablets (pharma)</td>
<td>Thane, India</td>
<td>OLPhe</td>
</tr>
<tr>
<td>PPW</td>
<td>Blister-packed tablets (pharma)</td>
<td>Chennai, India</td>
<td>PhEx, Stmul, Trust, ClFr</td>
</tr>
<tr>
<td>K. Sekar</td>
<td>Blister-packed tablets (pharma)</td>
<td>Villupuram, India</td>
<td>WldPh</td>
</tr>
<tr>
<td>Rhine Inc.</td>
<td>Blister-packed tablets (pharma)</td>
<td>Than, India</td>
<td>RxPrm, DrgRev</td>
</tr>
<tr>
<td>Supreme Suppliers</td>
<td>Blister-packed tablets (pharma)</td>
<td>Mumbai, India</td>
<td>Eva</td>
</tr>
<tr>
<td>Chen Hua</td>
<td>Small white plastic bottles (herbal)</td>
<td>Jiangmen, China</td>
<td>Eva</td>
</tr>
<tr>
<td>Etech Media Ltd</td>
<td>Novelty-sized supplement (herbal)</td>
<td>Christchurch, NZ</td>
<td>Staln</td>
</tr>
<tr>
<td>Herbal Health Fulfillment Warehouse</td>
<td>White plastic bottle (herbal)</td>
<td>MA, USA</td>
<td>Eva</td>
</tr>
<tr>
<td>MK Sales</td>
<td>White plastic bottle (herbal)</td>
<td>WA, USA</td>
<td>GlvMd</td>
</tr>
<tr>
<td>Riverton, Utah shipper</td>
<td>White plastic bottle (herbal)</td>
<td>UT, USA</td>
<td>DrMax, Grow</td>
</tr>
<tr>
<td>Guo Zhonglei</td>
<td>Foam-wrapped replica watch</td>
<td>Baoding, China</td>
<td>Dstn, UltRp</td>
</tr>
</tbody>
</table>

Table VI: List of product suppliers and associated affiliate programs and/or store brands.
### Acquiring banks

<table>
<thead>
<tr>
<th>Bank Name</th>
<th>BIN</th>
<th>Country</th>
<th>Affiliate Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azerigazbank</td>
<td>404610</td>
<td>Azerbaijan</td>
<td>GlvMd, RxPmr, PhEx, Stmul, RxPrn, WldPh</td>
</tr>
<tr>
<td>B&amp;N</td>
<td>425175</td>
<td>Russia</td>
<td>ASR</td>
</tr>
<tr>
<td>B&amp;S Card Service</td>
<td>490763</td>
<td>Germany</td>
<td>MaxGm</td>
</tr>
<tr>
<td>Borgun Hf</td>
<td>423262</td>
<td>Iceland</td>
<td>Trust</td>
</tr>
<tr>
<td>Canadian Imperial Bank of Commerce</td>
<td>452551</td>
<td>Canada</td>
<td>WldPh</td>
</tr>
<tr>
<td>Cartu Bank</td>
<td>478765</td>
<td>Georgia</td>
<td>DrgRev</td>
</tr>
<tr>
<td>DnB Nord (Pirma)</td>
<td>492175</td>
<td>Latvia</td>
<td>Eva, OLPh, USHC</td>
</tr>
<tr>
<td>Latvia Savings</td>
<td>490849</td>
<td>Latvia</td>
<td>EuSft, OEM, WchSh, Royal, SftSl</td>
</tr>
<tr>
<td>Latvijas Pasta Banka</td>
<td>489431</td>
<td>Latvia</td>
<td>SftSl</td>
</tr>
<tr>
<td>St. Kitts &amp; Nevis Anguilla National Bank</td>
<td>427852</td>
<td>St. Kitts &amp; Nevis</td>
<td>DmdRp, VgREX, Dstn, Luxry, SwsRp, OneRp</td>
</tr>
<tr>
<td>State Bank of Mauritius</td>
<td>474140</td>
<td>Mauritius</td>
<td>DrgRev</td>
</tr>
<tr>
<td>Visa Iceland</td>
<td>450744</td>
<td>Iceland</td>
<td>Staln</td>
</tr>
<tr>
<td>Wells Fargo</td>
<td>449215</td>
<td>USA</td>
<td>Green</td>
</tr>
<tr>
<td>Wirecard AG</td>
<td>424500</td>
<td>Germany</td>
<td>ClFr</td>
</tr>
</tbody>
</table>

Table V: Merchant banks authorizing or settling transactions for spam-advertised purchases, their Visa-assigned Bank Identification Number (BIN), their location, and the abbreviation used in Table IV for affiliate program and/or store brand.
So how much are spambots making?

• To understand, we would have to know:
  • Order volume (how much is sold as a result of an affiliate program over time?)
  • Purchasing behavior (what are people buying?)

• Turns out you can infer these
Predicting order volume

• Most affiliate programs provide a confirmation page with an order number

• This order number usually just increments
Predicting order volume

- Most affiliate programs provide a confirmation page with an order number

- This order number usually just increments

<table>
<thead>
<tr>
<th>Order ID</th>
<th>Jan 5</th>
<th>Jan 15</th>
<th>Jan 25</th>
<th>Feb 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx-promo</td>
<td>455 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pharmax</td>
<td>261 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glammed</td>
<td>582 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eurosoft</td>
<td>749 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33drugs</td>
<td>323 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>softsales</td>
<td>49 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>royal</td>
<td>443 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>online</td>
<td>192 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eva</td>
<td>887 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4rx</td>
<td>263 id/day</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Inferring what people buy

• EvaPharmacy (a top 5 spam-advertised pharmacy affiliate program):
  • 2/3 of outsourced image hosting was to compromised 3rd party servers

• They contacted the owners of these servers and asked for logs

• Correlated image logs with purchases
Figure 5: How a user interacts with an EvaPharmacy Web site, beginning with the landing page and then proceeding to a product page and the shopping cart. The main Web site contains embedded images hosted on separate compromised systems. When a browser visits such pages, the referrer information is sent to the image hosting servers for every new image visited.
### Affiliate profit

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>33drugs</td>
<td>9,862</td>
<td>$100</td>
<td>$980,000</td>
<td>$45.00</td>
<td>$440,000</td>
<td>$57.25</td>
<td>$560,000</td>
</tr>
<tr>
<td>4RX</td>
<td>8,001</td>
<td>$100</td>
<td>$800,000</td>
<td>$34.50</td>
<td>$280,000</td>
<td>$95.00</td>
<td>$760,000</td>
</tr>
<tr>
<td>EuroSoft</td>
<td>22,776</td>
<td>N/A</td>
<td>N/A</td>
<td>$26.50</td>
<td>$600,000</td>
<td>$84.50</td>
<td>$1,900,000</td>
</tr>
<tr>
<td>EvaPharmacy</td>
<td>26,962</td>
<td>$100</td>
<td>$2,700,000</td>
<td>$50.50</td>
<td>$1,300,000</td>
<td>$90.00</td>
<td>$2,400,000</td>
</tr>
<tr>
<td>GlavMed</td>
<td>17,933</td>
<td>$100</td>
<td>$1,800,000</td>
<td>$54.00</td>
<td>$970,000</td>
<td>$57.00</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Online Pharmacy</td>
<td>5,856</td>
<td>$100</td>
<td>$590,000</td>
<td>$37.00</td>
<td>$220,000</td>
<td>$58.00</td>
<td>$340,000</td>
</tr>
<tr>
<td>Pharmacy Express</td>
<td>7,933</td>
<td>$100</td>
<td>$790,000</td>
<td>$51.00</td>
<td>$410,000</td>
<td>$58.75</td>
<td>$460,000</td>
</tr>
<tr>
<td>Royal Software</td>
<td>13,483</td>
<td>N/A</td>
<td>N/A</td>
<td>$55.25</td>
<td>$750,000</td>
<td>$133.75</td>
<td>$1,800,000</td>
</tr>
<tr>
<td>Rx–Promotion</td>
<td>6,924</td>
<td>$100</td>
<td>$690,000</td>
<td>$45.00</td>
<td>$310,000</td>
<td>$57.25</td>
<td>$400,000</td>
</tr>
<tr>
<td>SoftSales</td>
<td>1,491</td>
<td>N/A</td>
<td>N/A</td>
<td>$20.00</td>
<td>$30,000</td>
<td>$134.50</td>
<td>$200,000</td>
</tr>
</tbody>
</table>

Table 4: Estimated monthly order volume, average purchase price, and monthly revenue (in dollars) per affiliate program using three different per-order price approximations.

Over 100k orders/month in this dataset alone

Some have guessed that “spammers make little money at all”
So who’s actually buying this junk?
So who’s actually buying this junk?

Figure 6: The geographic distribution of those who added an item to their shopping cart.

<table>
<thead>
<tr>
<th>Country</th>
<th>Visits</th>
<th>Cart Additions</th>
<th>Added Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>517,793</td>
<td>3,707</td>
<td>0.72%</td>
</tr>
<tr>
<td>Canada</td>
<td>50,234</td>
<td>218</td>
<td>0.43%</td>
</tr>
<tr>
<td>Philippines</td>
<td>42,441</td>
<td>39</td>
<td>0.09%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>39,087</td>
<td>131</td>
<td>0.34%</td>
</tr>
<tr>
<td>Spain</td>
<td>26,968</td>
<td>59</td>
<td>0.22%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>26,661</td>
<td>31</td>
<td>0.12%</td>
</tr>
<tr>
<td>France</td>
<td>18,541</td>
<td>37</td>
<td>0.20%</td>
</tr>
<tr>
<td>Germany</td>
<td>15,726</td>
<td>56</td>
<td>0.36%</td>
</tr>
<tr>
<td>Australia</td>
<td>15,101</td>
<td>86</td>
<td>0.57%</td>
</tr>
<tr>
<td>India</td>
<td>10,835</td>
<td>17</td>
<td>0.16%</td>
</tr>
<tr>
<td>China</td>
<td>8,924</td>
<td>30</td>
<td>0.34%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>8,363</td>
<td>21</td>
<td>0.25%</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>8,266</td>
<td>36</td>
<td>0.44%</td>
</tr>
<tr>
<td>Mexico</td>
<td>7,775</td>
<td>17</td>
<td>0.22%</td>
</tr>
<tr>
<td>Singapore</td>
<td>7,586</td>
<td>17</td>
<td>0.22%</td>
</tr>
</tbody>
</table>

Table 2: The top 15 countries and the percentage of visitors who added an item to their shopping cart.
So who’s actually buying this junk?

Stop buying this junk!

Figure 6: The geographic distribution of those who added an item to their shopping cart.

<table>
<thead>
<tr>
<th>Country</th>
<th>Visits</th>
<th>Cart Additions</th>
<th>Added Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>517,793</td>
<td>3,707</td>
<td>0.72%</td>
</tr>
<tr>
<td>Canada</td>
<td>50,234</td>
<td>218</td>
<td>0.43%</td>
</tr>
<tr>
<td>Philippines</td>
<td>42,441</td>
<td>39</td>
<td>0.09%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>39,087</td>
<td>131</td>
<td>0.34%</td>
</tr>
<tr>
<td>Spain</td>
<td>26,968</td>
<td>59</td>
<td>0.22%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>26,661</td>
<td>31</td>
<td>0.12%</td>
</tr>
<tr>
<td>France</td>
<td>18,541</td>
<td>37</td>
<td>0.20%</td>
</tr>
<tr>
<td>Germany</td>
<td>15,726</td>
<td>56</td>
<td>0.36%</td>
</tr>
<tr>
<td>Australia</td>
<td>15,101</td>
<td>86</td>
<td>0.57%</td>
</tr>
<tr>
<td>India</td>
<td>10,835</td>
<td>17</td>
<td>0.16%</td>
</tr>
<tr>
<td>China</td>
<td>8,924</td>
<td>30</td>
<td>0.34%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>8,363</td>
<td>21</td>
<td>0.25%</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>8,266</td>
<td>36</td>
<td>0.44%</td>
</tr>
<tr>
<td>Mexico</td>
<td>7,775</td>
<td>17</td>
<td>0.22%</td>
</tr>
<tr>
<td>Singapore</td>
<td>7,586</td>
<td>17</td>
<td>0.22%</td>
</tr>
</tbody>
</table>

Table 2: The top 15 countries and the percentage of visitors who added an item to their shopping cart.
What are you buying?

<table>
<thead>
<tr>
<th>Product</th>
<th>Quantity</th>
<th>Min order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic Viagra</td>
<td>568</td>
<td>$78.80</td>
</tr>
<tr>
<td>Cialis</td>
<td>286</td>
<td>$78.00</td>
</tr>
<tr>
<td>Cialis/Viagra Combo Pack</td>
<td>172</td>
<td>$74.95</td>
</tr>
<tr>
<td>Viagra Super Active+</td>
<td>121</td>
<td>$134.80</td>
</tr>
<tr>
<td>Female (pink) Viagra</td>
<td>119</td>
<td>$44.00</td>
</tr>
<tr>
<td>Human Growth Hormone</td>
<td>104</td>
<td>$83.95</td>
</tr>
<tr>
<td>Soma (Carisoprodol)</td>
<td>99</td>
<td>$94.80</td>
</tr>
<tr>
<td>Viagra Professional</td>
<td>87</td>
<td>$139.80</td>
</tr>
<tr>
<td>Levitra</td>
<td>83</td>
<td>$100.80</td>
</tr>
<tr>
<td>Viagra Super Force</td>
<td>81</td>
<td>$88.80</td>
</tr>
<tr>
<td>Cialis Super Active+</td>
<td>72</td>
<td>$172.80</td>
</tr>
<tr>
<td>Amoxicillin</td>
<td>47</td>
<td>$35.40</td>
</tr>
<tr>
<td>Lipitor</td>
<td>38</td>
<td>$14.40</td>
</tr>
<tr>
<td>Ultram</td>
<td>38</td>
<td>$45.60</td>
</tr>
<tr>
<td>Tramadol</td>
<td>36</td>
<td>$82.80</td>
</tr>
<tr>
<td>Prozac</td>
<td>35</td>
<td>$19.50</td>
</tr>
<tr>
<td>Cialis Professional</td>
<td>33</td>
<td>$176.00</td>
</tr>
<tr>
<td>Retin A</td>
<td>31</td>
<td>$47.85</td>
</tr>
</tbody>
</table>
“Why do you rob banks?”
“Because that’s where the money is”

Why does the emergence of the underground economy matter?

- Many of the centralized components of these networks get pursued and shut down
- Markets lead to efficiencies and specializations
  - Lowers barrier to entry: only need a single skill
  - Some underground market activities are legal
- Competition spurs innovation
  - Accelerates the arms race
  - Defenders must assume a more pessimistic threat model
- Facilitates non-$ Internet attacks
  - Provides actors (political, nation-state) with cheap attack components
Why studying it matters

And why *continuing* to study it matters

- Like any complex system, these markets can themselves be infiltrated
  - Some research on infiltrating affiliate programs & botnets, taking over C&C

- Can identify choke points
  - Many hosting services have been shut down
  - Draws attention to shady banks
  - Draws attention to shady doctors
    - Early spambot had one doctor writing 1500+ prescriptions per day
Some final thoughts on security

• It’s difficult

• It requires demystification of the services you use, deep knowledge of the tools you use, and adherence to a set of design principles

• It requires vigilance—attackers won’t rest, so neither can we
Some final thoughts on security

• It’s fun!

• Constant race for innovation, often surprising turns
  • But sometimes just frustrating mistakes

• It permeates all aspects of computer science, system building, human interaction, ….
What I want from all of you
What I want from all of you

You are now responsible.
What I want from all of you

You are now responsible.

Bring copious amounts of thoroughness, responsibility, ethics, and education to your future endeavors.