Cybercrime

INGI2347: COMPUTER SYSTEM SECURITY (Spring 2016)

Marco Canini

Université catholique de Louvain

Lecture slides adapted from Upenn CSE331 by Steve Zdancewic and UC Berkeley CS161 by Vern Paxson
Reproduced with permission

Outline

- Distributed DoS (DDoS)
- Botnets
- Spam & Spam Profit
- The Rise of the Underground Economy

Distributed DoS (DDoS)

Attacks on Availability

- Denial-of-Service (DoS, or "*doss*"): *keeping someone from using a computing service*
- How broad is this sort of threat?
  - *Very*: **huge** attack surface
- We do though need to consider our threat model …
  - What might motivate a DoS attack?

Motivations for DoS

- Showing off / entertainment / ego
- Competitive advantage
  - Maybe commercial, maybe just to win
- Vendetta / denial-of-money
- Extortion
- Political statements
- Impair defenses
- Espionage
- Warfare

Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen ✉ February 4, 2009 | 12:13 pm | Categories: Cybarmageddon!

What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.

Cyberattack on Hong Kong Vote Was Among Largest Ever, Security Chief Says

By ALAN WONG JUNE 21, 2014 10:01 AM 3 Comments

Email

Share

Tweet

Save

More

The online voting platform for the unofficial referendum now underway on Hong Kong's political future has been subjected to one of the most severe cyberattacks of its kind ever seen, according to the head of the Internet security company tasked with protecting it.

Matthew Prince, chief executive and co-founder of the San Francisco-based company CloudFlare, said in an email Friday that the distributed denial-of-service attack (also known as DDoS) on Occupy Central's voting platform was "one of the largest and most persistent" ever.

http://nyti.ms/1leJtEd

Attacks on Availability

- Denial-of-Service (DoS, or "*doss*"): *keeping someone from using a computing service*
- How broad is this sort of threat?
  - *Very*: **huge** attack surface
- We do though need to consider our threat model …
  - What might motivate a DoS attack?
- Two basic approaches available to an attacker:
  - Deny service via a **program flaw** ("`*NULL`")
    - E.g., supply an input that crashes a server or cause system shutdown
  - Deny service via **resource exhaustion** ("`while(1);`")
    - E.g., consume CPU, memory, disk, network

DoS Defense in General Terms

- Defending against program flaws requires:
  - Careful *authentication*
    - Don't obey shut-down orders from imposters
  - Careful coding/testing/review
  - Consideration of behavior of defense mechanisms
    - E.g. buffer overflow detector that when triggered halts execution to prevent code injection ⇒ denial-of-service
- Defending resources from exhaustion can be **really** hard. Requires:
  - *Isolation mechanisms*
    - Keep adversary's consumption from affecting others
  - *Reliable identification* of different users
    - Know who the adversary is in the first place!

DoS & Operating Systems

- How could you DoS a multi-user Unix system on which you have a login?
  - `# rm -rf /`
    - (if you have root - but then just "halt" works well!)
  -
```
char buf[1024];
int f = open("/tmp/junk");
while (1) write(f, buf, sizeof(buf));
```
    - Gobble up all the disk space!
  - `while (1) fork();`
    - Create a zillion processes!
  - Create zillions of files, keep opening, reading, writing, deleting
    - Thrash the disk
  - … doubtless many more
- Defenses?
  - Isolate users / impose quotas

DoS & Networks

- How could you DoS a target's Internet access?
  - Send a zillion packets at them
  - Internet lacks isolation between traffic of different users!
- What resources does attacker need to pull this off?
  - At least as much sending capacity ("bandwidth") as the bottleneck link of the target's Internet connection
    - Attacker sends maximum-sized packets
  - **Or**: overwhelm the rate at which the bottleneck router can process packets
    - Attacker sends minimum-sized packets!
      - (in order to maximize the packet arrival rate)

Defending Against Network DoS

- Suppose an attacker has access to a beefy system with high-speed Internet access (a "big pipe")
- They pump out packets towards the target at a very high rate
- What might the target do to defend against the onslaught?
  - Install a network filter to discard any packets that arrive with attacker's IP address as their source
    - E.g., `drop * 66.31.1.37:* -> *:*`
    - Or it can leverage *any other pattern* in the flooding traffic that's not in benign traffic
  - Filter = *isolation mechanism*
  - Attacker's IP address = means of *identifying* misbehaving user

Filtering Sounds Pretty Easy …

- … but it's not. What steps can the attacker take to defeat the filtering?
  - Make traffic appear as though it's from many hosts
    - Spoof the source address so it can't be used to filter
      - Just pick a random 32-bit number of each packet sent
    - How does a defender filter this?
      - They don't!
      - Best they can hope for is that operators around the world implement anti-spoofing mechanisms (today about 75% do)
  - Use many hosts to send traffic rather than just one
    - Distributed Denial-of-Service = **DDoS** ("dee-doss")
    - Requires defender to install complex filters
    - How many hosts is "enough" for the attacker?
      - Today they are very cheap to acquire … :-(

It's Not A "Level Playing Field"

- When defending resources from exhaustion, need to beware of asymmetries, where attackers can consume victim resources with little comparable effort
  - Makes DoS easier to launch
  - Defense costs much more than attack

- Particularly dangerous form of asymmetry: **amplification**
  - Attacker leverages system's own structure to pump up the load they induce on a resource

Amplification:Network DoS

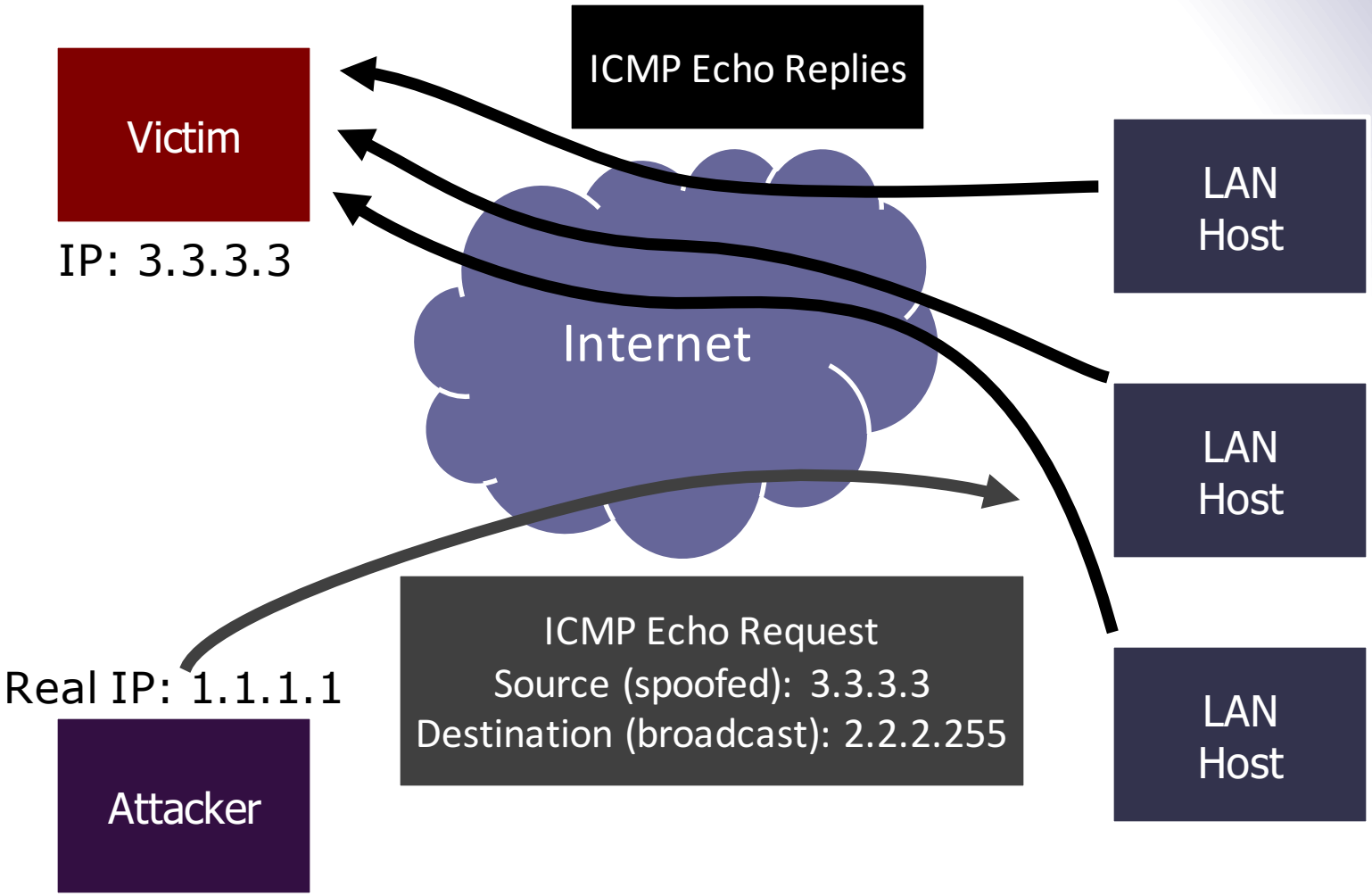
- One technique for magnifying flood traffic: leverage Internet's *broadcast functionality*

Amplification: Network DoS

- One technique for magnifying flood traffic: leverage Internet's *broadcast functionality*
- How does an attacker exploit this?
  - Send traffic to the broadcast address and spoof it *as though the DoS victim sent it*
  - All of the replies then go to the victim rather than the attacker's machine
  - Each attacker pkt yields dozens of flooding pkts

smurf attack

Smurf Example



Amplification:Network DoS

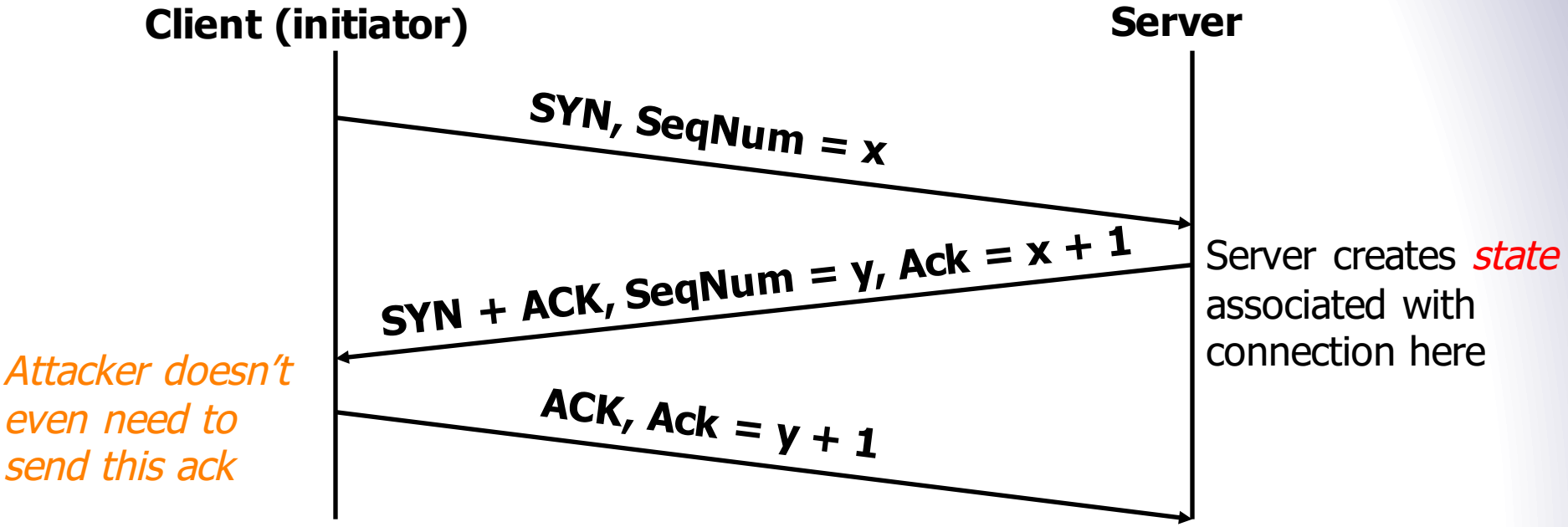
- One technique for magnifying flood traffic: leverage Internet's *broadcast functionality*
- How does an attacker exploit this?
  - Send traffic to the broadcast address and spoof it *as though the DoS victim sent it*
  - All of the replies then go to the victim rather than the attacker's machine
  - Each attacker pkt yields dozens of flooding pkts

smurf attack

- Another example: DNS lookups
  - *Reply is often much bigger than request*
  - So attacker spoofs request seemingly from the target
    - Small attacker packet yields large flooding packet

Transport-Level Denial-of-Service

- Recall TCP's 3-way connection handshake
  - Goal: agree on initial sequence numbers
- So a single SYN from an attacker suffices to force the server to *spend some memory*



TCP SYN Flooding

- Attacker targets *memory* rather than network capacity
- Every (unique) SYN that the attacker sends burdens the target
- What should target do when it has no more memory for a new connection?
- No good answer!
  - *Refuse* new connection?
    - Legit new users can't access service
  - *Evict* old connections to make room?
    - Legit old users get kicked off

TCP SYN Flooding

- How can the target defend itself?

- Approach #1: make sure they have **tons of memory**!
  - How much is enough? Depends on resources attacker can bring to bear

TCP SYN Flooding

- Approach #2: identify bad actors & refuse their connections
  - Hard because only way to identify them is based on IP address
    - We can't for example require them to send a password because doing so requires we have an established connection!
  - For a public Internet service, who knows which addresses customers might come from?
  - Plus: attacker can spoof addresses since they don't need to complete TCP 3-way handshake
- Approach #3: don't keep state! ("*SYN cookies*"; *only works for spoofed SYN flooding*)

TCP SYN Flooding

- Approach #4: spread service across lots of different physical servers
  - This is a **general defense** against a wide range of DoS threats (including application-layer)
  - If servers are at different places around the network, protects against *network-layer* DoS too
- But: costs $$
- And: some services are not easy to divide up
  - Such as when need to modify common database

Application-Layer DoS

- Rather than exhausting network or memory resources, attacker can overwhelm a service's processing capacity

- There are many ways to do so, often at little expense to attacker compared to target (*asymmetry*)

The link sends a request to the web server that requires heavy processing by its "backend database"

(Such queries are usually written in a language called SQL, as we'll see next lecture)

Application-Layer DoS

- Rather than exhausting network or memory resources, attacker can overwhelm a service's processing capacity
- There are many ways to do so, often at little expense to attacker compared to target (asymmetry)
- Defenses against such attacks?
- Approach #1: Only let legit users to issue expensive requests
  - Relies on being able to identify/authenticate them (e.g., CAPTCHAs)
  - Note: that *this itself might be expensive*!
- Approach #2: Look for clusters of similar activity
  - Arms race with attacker AND costs *collateral damage*
- Approach #3: distribute service across multiple servers ($$$)

DDoS Recent Examples

- Jun 2014 – Hong Kong's Occupy Central voting platform hit by 300+ Gbps DDoS
- Feb 2014 – 400 Gbps NTP amplification DDoS attack against an organization in Europe
- Mar 2013 – 300 Gbps DDoS attack against Spamhaus
- Oct 2012 – HSBC experienced a downtime of many of its website worldwide
- Aug 2012 – WikiLeaks was hit by a DDoS attack
- Jun 2012 – CIA website fallen foul of a DDoS attack
- Mar 2011 – WordPress.com suffered a large DDoS attack

Akamai's State of the Internet Report

	Country/Region	Q4 '13 Traffic %	Q3 '13 %
1	China	43%	35%
2	United States	19%	11%
3	Canada	10%	0.4%
4	Indonesia	5.7%	20%
5	Taiwan	3.4%	5.2%
6	Netherlands	2.7%	0.5%
7	Russia	1.5%	2.6%
8	Brazil	1.1%	2.1%
9	Romania	0.9%	1.7%
10	Germany	0.8%	0.9%
–	Other	12%	17%

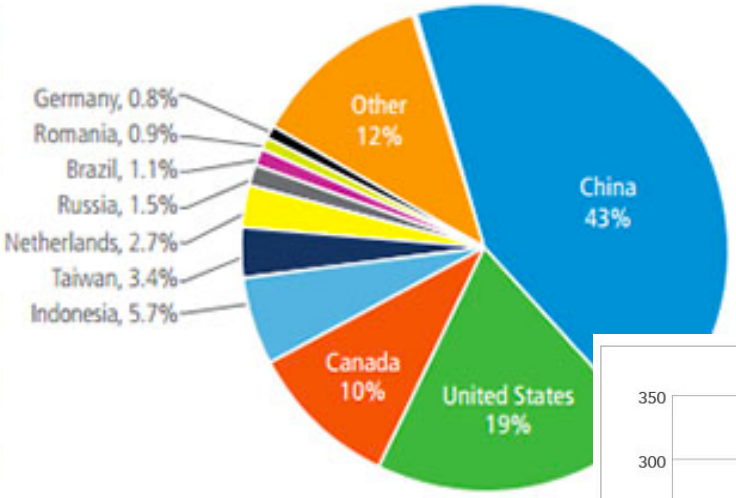


Figure 1: Attack Traffic, Top Originating Countries (by source IP address, not attribution)

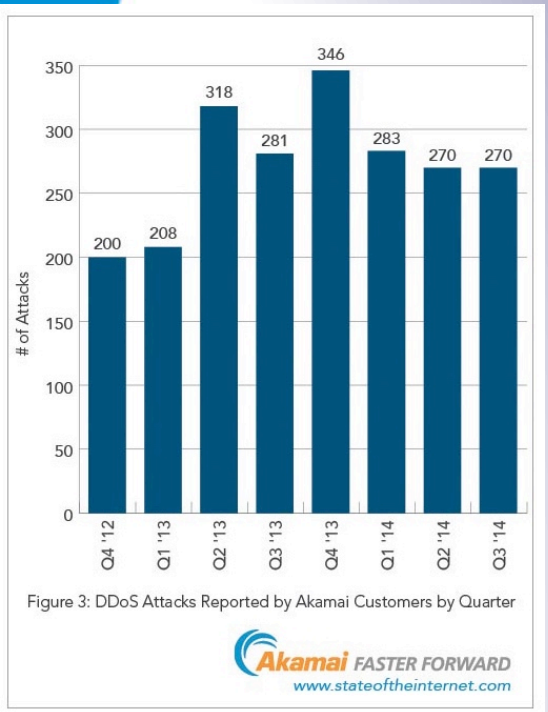
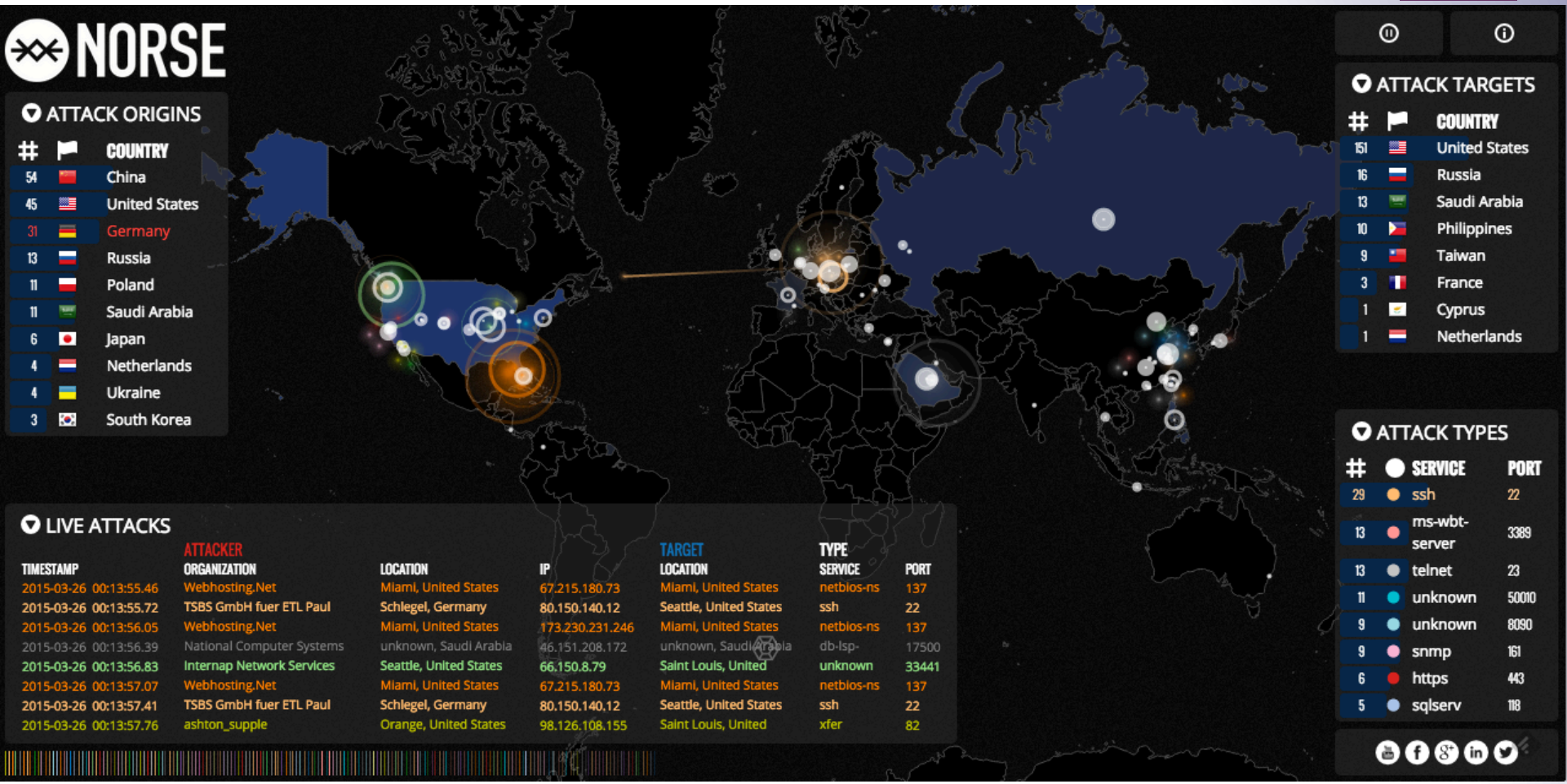


Figure 3: DDoS Attacks Reported by Akamai Customers by Quarter

Let's watch some live attacks …

http://map.ipviking.com/

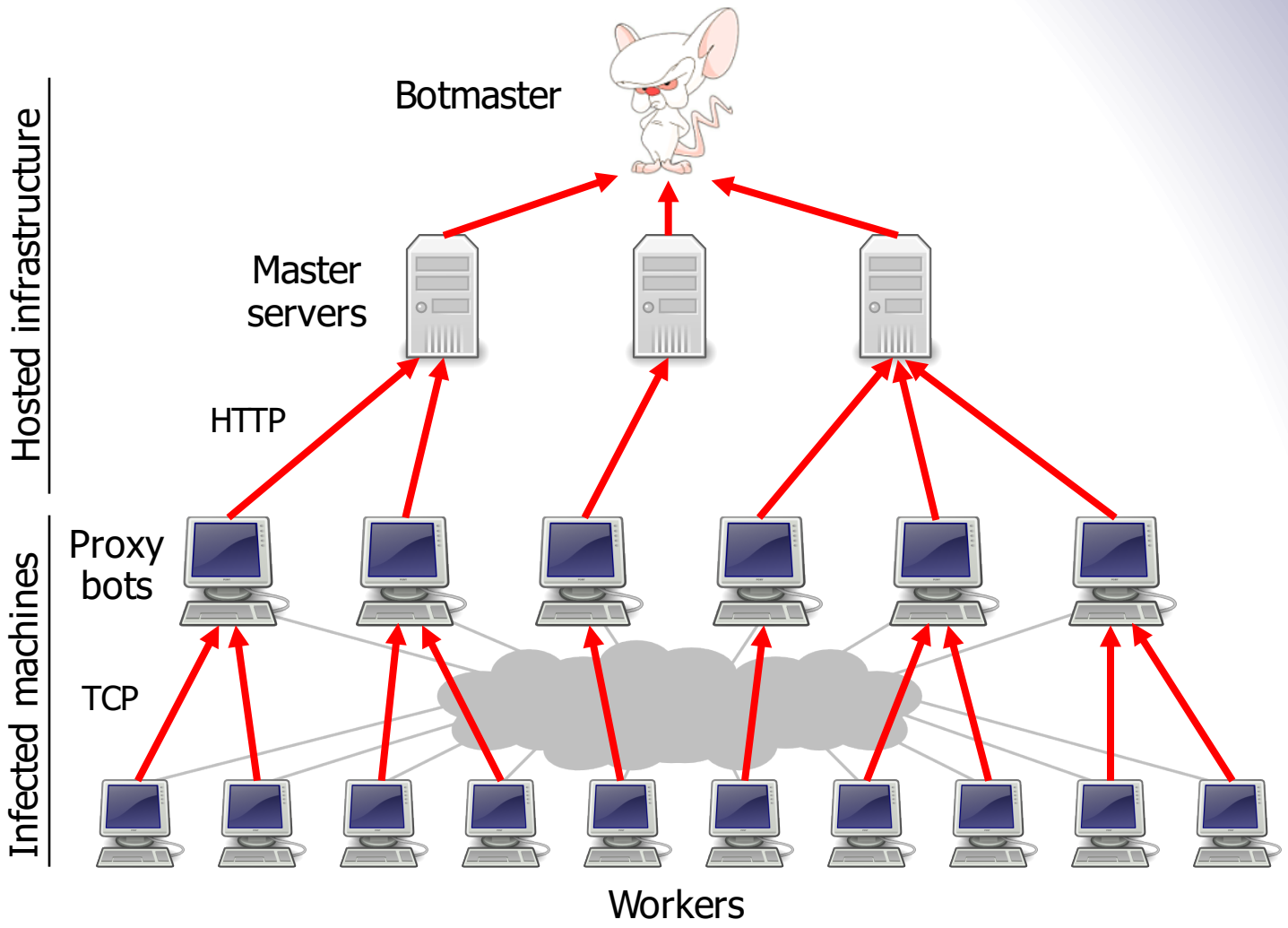


Botnets

Botnets

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

The Storm Botnet



Example of C&C Messages

1. Activation (report from bot to botmaster)
2. Email address harvests
3. Spamming instructions
4. Delivery reports
5. DDoS instructions
6. FastFlux instructions (rapidly changing DNS)
7. HTTP proxy instructions
8. Sniffed passwords report
9. IFRAME injection/report

From the "Storm" botnet ~2008

Fighting Bots / Botnets

- How can we defend against bots / botnets?

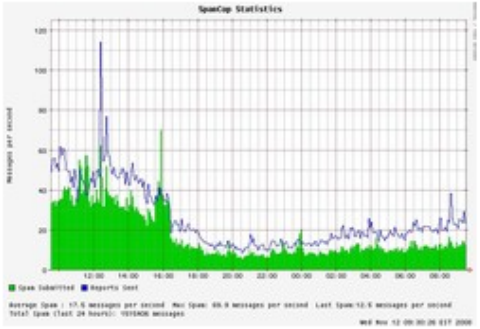
- Approach #1: prevent the initial bot infection
  - Equivalent to preventing malware infections in general …. HARD
- Approach #2: take down the C&C master server
  - Find its IP address, get associated ISP to pull plug

Security Fix

Brian Krebs on Computer Security

Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (**Note**: A link to the full story on McColo's demise is available here.)



Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

> In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic shows a similar decline, from about 40 spam e-

Fighting Bots / Botnets

- How can we defend against bots / botnets?

- Approach #1: prevent the initial bot infection
  - Equivalent to preventing malware infections in general …. HARD
- Approach #2: Take down the C&C master server
  - Find its IP address, get associated ISP to pull plug
- Botmaster countermeasures?
  - Counter #1: keep moving around the master server
    - Bots resolve a domain name to find it (e.g. `c-and-c.evil.com`)
    - Rapidly alter address associated with name ("fast flux")
  - Counter #2: buy off the ISP …

Fighting Bots / Botnets

- Approach #3: seize the domain name used for C&C
  - This is what's currently often used, often to good effect …
- … Botmaster counter-measure?
  - Each day (say), bots generate large list of possible domain names using a Domain Generation Algorithm
    - Large = 50K, in some cases
  - Bots then try a random subset looking for a C&C server
    - Server **signs** its replies, so bot can't be duped
    - Attacker just needs to hang on to a small portion of names to retain control over botnet
  - This is becoming state-of-the-art …
- Counter-counter measure?
  - Behavioral signature: look for hosts that make a lot of failed DNS lookups (research)

Addressing The Botnet Problem

- What are our prospects for securing the Internet from the threat of botnets? What angles can we pursue?
- Angle #1: detection/cleanup
  - Detecting infection of individual bots hard as it's the *defend-against-general-malware* problem
  - Detecting bot doing C&C likely a losing battle as attackers improve their sneakiness & crypto
  - Cleanup today lacks oomph:
    - **Who's responsible?** … and do they **care**? (*externalities*)
    - Landscape could greatly change with different model of liability
- Angle #2: go after the C&C systems / botmasters
  - Difficult due to ease of Internet anonymity & complexities of international law
    - But: a number of recent successes in this regard
  - One promising angle: policing domain name registrations

Addressing The Problem

- Angle #3: prevention
  - Bots require installing new executables or modifying existing ones
  - Perhaps via infection …
    - … or perhaps just via user being fooled / imprudent
- Better models?
- We could lock down systems so OS prohibits user from changing configuration
  - Sacrifices flexibility
  - How does this work for home users?
  - Can we leverage trusted kernels + white lists / code signing?
- Or: structure OS/browser so code runs with Least Privilege
  - Does this solve the problem?
  - Depends on how granular the privileges are … and how the decision is made regarding just what privileges are "least"
    - E.g., iTunes App Store model (vetting), Android model (user confirmation)

Spam & Spam Profit

Spam email

- Unsolicited automated email; sent in bulk to numerous recipients
  - (The sender is a stranger to the recipient)

The sender address is (almost) always forged to prevent counterattacks

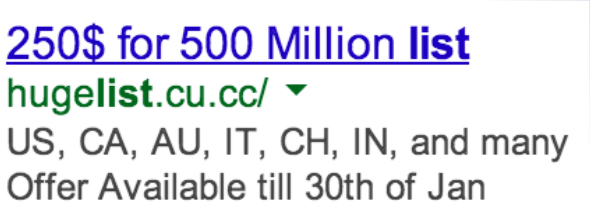
- Basic SMTP (Simple Mail Transfer Protocol) does not perform any verification of the sender's address, it is easy to forge mails

Spamming Techniques

- Method #1: Use of own/ISP SMTP server
- Method #2: Abuse of open relays
  - A single message sent to the mail server can be relayed to thousands of addresses
- Method #3: Abuse a webmail account
  - Create fake webmail accounts and send spam through them
- Method #4: Infect computers
  - Take control of infected computers to send spam

How do spammers harvest emails?

- Just buy a list of emails
- Crawl the Web
- Mailing lists & newsgroups
- Hack into a database
- Scan files on infected machines
- Hoax, scam and chain letters
- By guessing (dictionary, brute force, standard)



Stopping Spam

- Anti-Spam laws
  - Legislation to restrict use of email spam in several countries
- Protection via a technical solution
  - Filters
    - "I think it's possible to stop spam, and that content-based filters are the way to do it. The Achilles heel of the spammers is their message. They can circumvent any other barrier you set up. They have so far, at least. But they have to deliver their message, whatever it is. If we can write software that recognizes their messages, there is no way they can get around that" – Paul Graham, 2002
  - Black/white/grey lists

Filters

- Feature-recognizing filters
  - Rules that recognize individual properties of spam
    - E.g. mentions "Viagra", has all uppercase subject, etc.
  - Assign a spam "score" to email
  - How many points should an email get for having the word "drug" in it?
- Statistical filtering based on the Bayesian approach
  - Proposed by Paul Graham in 2002 (http://www.paulgraham.com/spam.html)
  - Trained on user's email labeled as spam vs. not spam
  - Assigns each message with a probability of being spam
- Filters are not perfect and cannot prevent false positives or false negatives

Black/White/Grey Lists

- Servers use lists to decide the acceptance of emails
- E.g. Spamhaus SBL and XBL lists
  - http://www.spamhaus.org/
  - SBL: IPs of known spam operators
  - XBL: IPs of hijacked systems relying spams
- Challenges:
  - Maintain lists up to date
  - Whitelisting requires senders to be known a priori
  - Greylisting (block a mail if the behavior of the sender's server is abnormal) introduces delivery delays (while user behavior is checked)

Monetizing Spam

- In what different ways can spammers make money off of sending spam?
  - And who has incentives to thwart these schemes?
    - (Other than law enforcement)
- Scheme #1: advertise goods or services
  - Examples: fake Rolexes, Viagra, university degrees
  - Profit angle: increased sales
  - Who'll try to stop: brand holders

Anatomy of a modern Pharma spam campaign

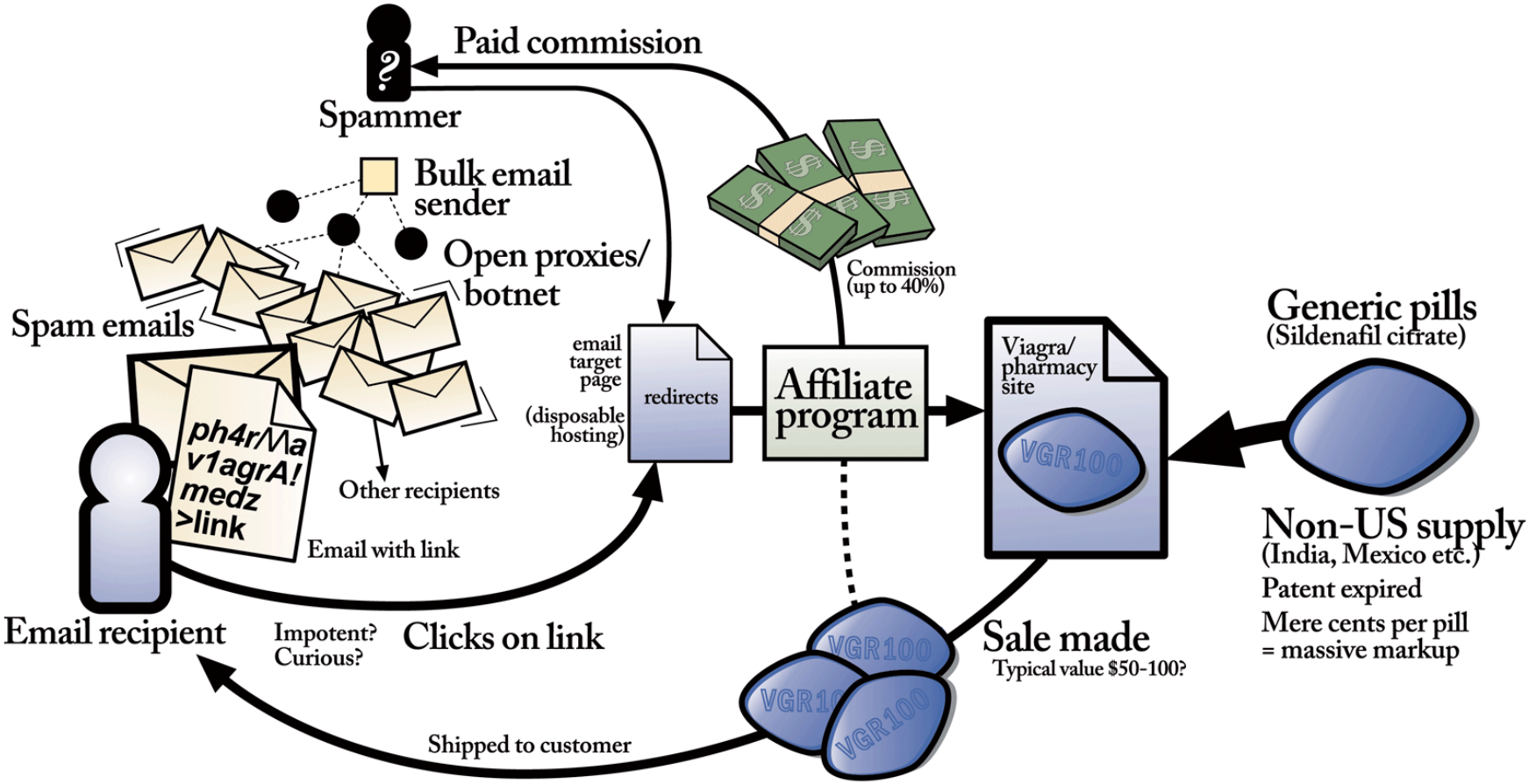


Diagram by Stuart Brown
http://modernlifeisrubbish.co.uk

Monetizing Spam

- In what different ways can spammers make money off of sending spam?
  - And who has incentives to thwart these schemes?
    - (Other than law enforcement)
- Scheme #1: advertise goods or services
  - Examples: fake Rolexes, Viagra, university degrees
  - Profit angle: increased sales
  - Who'll try to stop: brand holders
- Scheme #2: phishing
  - Profit angle: transfer $$$ out of accounts; sell accounts to others; use accounts for better spamming (e.g. Facebook)
  - Opponents: issuers of accounts
  - Note: targeted phishing ("spear-phishing") doesn't actually need much in the way of spam due to low volume

Monetizing Spam

- Scheme #3: scams
  - Examples: pen pal relationships, 419 (“Nigerian”)
  - Profit angle: con victim into sending money
  - Opponents: scambaiters (e.g., www.419eater.com)

- Scheme #4: recruiting crooks/underlings
  - Examples: money mules, re-shippers
  - Profit angle: enables profiting from cybercrime
  - Opponents: ?

Monetizing Spam

- Scheme #3: scams
  - Examples: pen pal relationships, 419 ("Nigerian")
  - Profit angle: c
  - Opponents: sc

Money mules take incoming (fraudulent) financial transfers to their bank accounts, wire-transfer 90% out of country, keep 10%

- Scheme #4: recruiting crooks/underlings
  - Examples: money mules, re-shippers
  - Profit angle: enables profiting from cybercrime
  - Opponents: ?

Monetizing Spam

- Scheme #3: scams
  - Examples: pen pal relationships, 419 ("Nigerian")
  - Profit angle: con victim i
  - Opponents: scambaiters

Re-shippers receive shipments of goods (e.g., a laptop bought using a stolen account) and re-mail them outside the country

- Scheme #4: recruiting crooks/underlings
  - Examples: money mules, re-shippers
  - Profit angle: enables profiting from cybercrime
  - Opponents: ?

Monetizing Spam

- Scheme #5: pump-and-dump
  - Example: "Falcon Energy (FPK) is about to go through the roof! Don't miss out on $eriou$ Profit$!"
  - Profit angle: penny-stock momentarily goes up, dump pre-bought shares when it does
  - Opponents: Securities and Exchange Commission
  - Note: unlike other monetization techniques, the "back channel" is out-of-band
    - No link in messages back to the scammer
- Scheme #6: recruiting bots
  - Examples: "important security patch!", "someone sent you a greeting card!"
  - Profit angle: get malware installed on new machines
  - Opponents: ?

The Rise of the Underground Economy

BuyAccs.com

BUY BULK ACCOUNTS AT BEST PRICES

Russian Version English Version

If you need quality **bulk accounts**, you've come to the right place. You can get your accounts **immediately** after your payment - there is no need to wait.

All the accounts are provided in **any format** you like. Just use our **free account converter** to get them in the way you need.

Special rates are applied if you purchase less than 1000 accounts.

We accept Paypal, Perfectmoney and Webmoney.

Please, review our terms and conditions before purchasing any accounts.

Earn Money Selling Accounts

Buy Yahoo Accounts
Buy Twitter Accounts
Buy Hotmail Accounts
Buy Tumblr Accounts
Buy Facebook Accounts

For sale

Provider	Quantity	Price for 1000 accounts
Gmail.com USA PVA	1360	1K-10K: **$100** | 10K-20K: **$100** | 20K+: **$100**
Yahoo.com USA PVA	6793	1K-10K: **$130** | 10K-20K: **$130** | 20K+: **$130**
Hotmail.com USA PVA	9058	1K-10K: **$120** | 10K-20K: **$120** | 20K+: **$120**
Hotmail.com Aged	13142	1K-10K: **$15** | 10K-20K: **$14** | 20K+: **$13**
Hotmail.com POP3	5417	1K-10K: **$10** | 10K-20K: **$9.5** | 20K+: **$9**
Hotmail.com Basic	7075	1K-10K: **$8** | 10K-20K: **$7.5** | 20K+: **$7**
Yahoo.com	96461	1K-10K: **$14** | 10K-20K: **$13** | 20K+: **$12**
Yahoo.com USA	31975	1K-10K: **$20** | 10K-20K: **$20** | 20K+: **$20**
Yahoo.com Basic	40826	1K-10K: **$10** | 10K-20K: **$9.5** | 20K+: **$9**

News

23 Mar 2015
New arrivals! Just added **Netcourrier.com** and **Seznam.cz** accounts with **POP3** enabled.

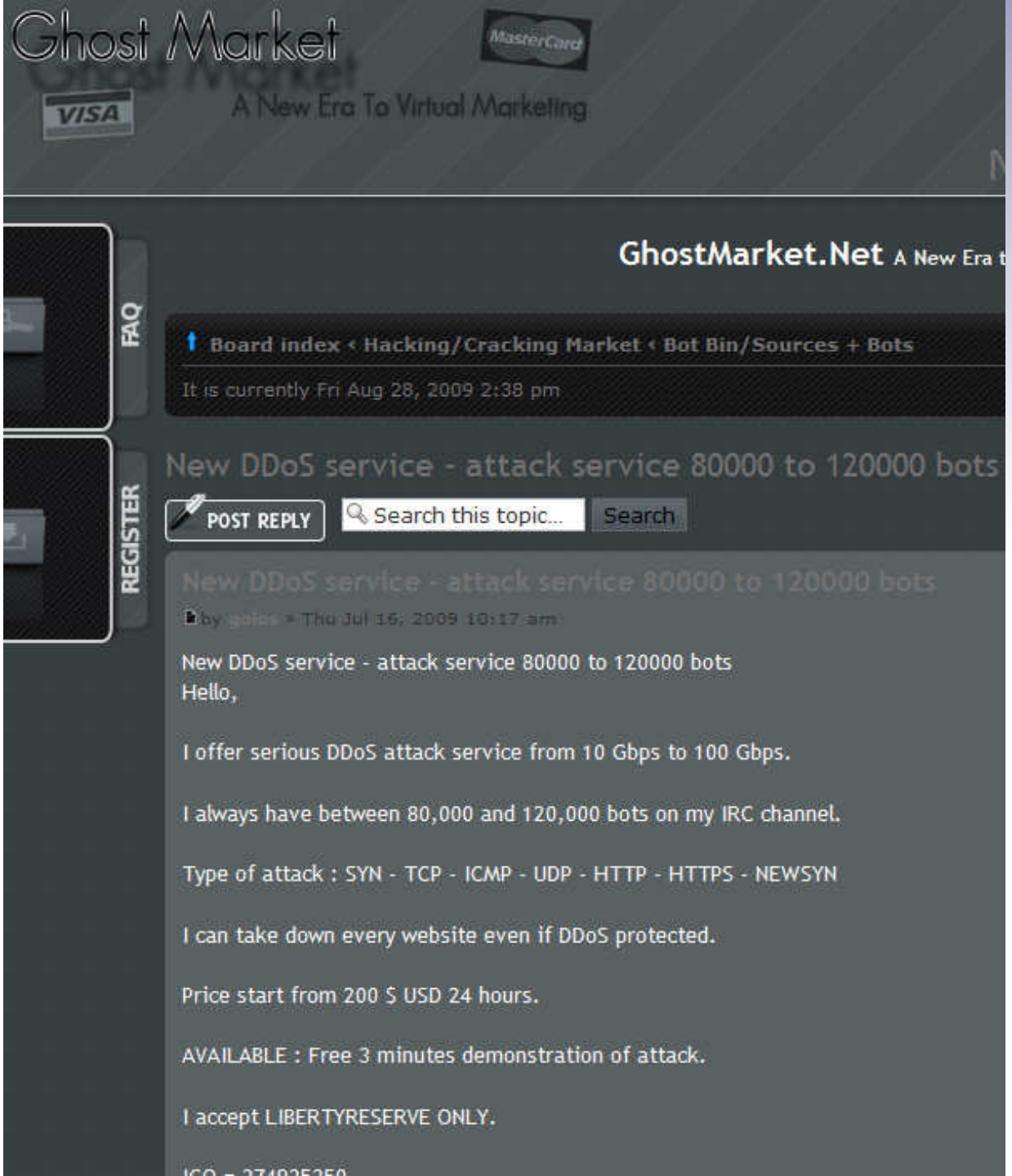
02 Mar 2015
Just added **Tinder PVA** accounts.

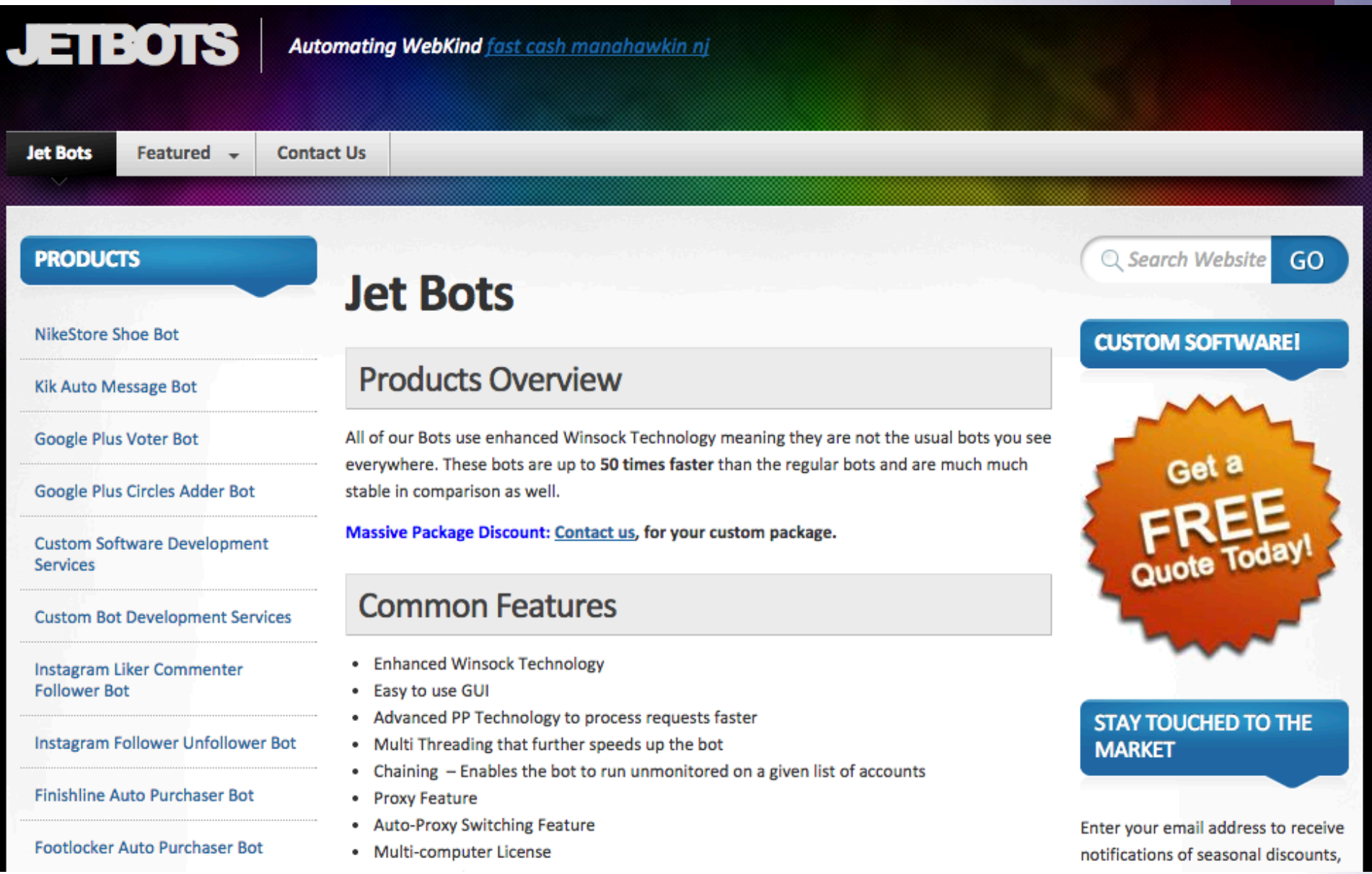
06 Dec 2014
You can now pay in **EUR** for any accounts. Choose **Paypal EUR** option during checkout.

24 Nov 2014
WMZ payments are **available** again.

23 Nov 2014
Important! **Yahoo.com Basic** accounts can be used with **POP3 only**! Please, **do NOT buy** them if you intend to use Web interface!

31 Oct 2014
You can see **account samples** before purchase. Just choose the accounts you need, and **we will show you what you will get** before you pay!


Ghost Market
MasterCard
VISA
A New Era To Virtual Marketing
FAQ
REGISTER
GhostMarket.Net A New Era t
Board index ‹ Hacking/Cracking Market ‹ Bot Bin/Sources + Bots
It is currently Fri Aug 28, 2009 2:38 pm
New DDoS service - attack service 80000 to 120000 bots
POST REPLY
Search this topic...
Search
New DDoS service - attack service 80000 to 120000 bots
by gales » Thu Jul 16, 2009 10:17 am
New DDoS service - attack service 80000 to 120000 bots
Hello,
I offer serious DDoS attack service from 10 Gbps to 100 Gbps.
I always have between 80,000 and 120,000 bots on my IRC channel.
Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN
I can take down every website even if DDoS protected.
Price start from 200 $ USD 24 hours.
AVAILABLE : Free 3 minutes demonstration of attack.
I accept LIBERTYRESERVE ONLY.


JETBOTS
Automating WebKind fast cash manahawkin nj
Jet Bots
Featured
Contact Us
PRODUCTS
NikeStore Shoe Bot
Kik Auto Message Bot
Google Plus Voter Bot
Google Plus Circles Adder Bot
Custom Software Development Services
Custom Bot Development Services
Instagram Liker Commenter Follower Bot
Instagram Follower Unfollower Bot
Finishline Auto Purchaser Bot
Footlocker Auto Purchaser Bot
Jet Bots
Products Overview
All of our Bots use enhanced Winsock Technology meaning they are not the usual bots you see everywhere. These bots are up to 50 times faster than the regular bots and are much much stable in comparison as well.
Massive Package Discount: Contact us, for your custom package.
Common Features
Enhanced Winsock Technology
Easy to use GUI
Advanced PP Technology to process requests faster
Multi Threading that further speeds up the bot
Chaining – Enables the bot to run unmonitored on a given list of accounts
Proxy Feature
Auto-Proxy Switching Feature
Multi-computer License
Search Website
GO
CUSTOM SOFTWARE!
Get a FREE Quote Today!
STAY TOUCHED TO THE MARKET
Enter your email address to receive notifications of seasonal discounts,

Underground Economy IRC Market

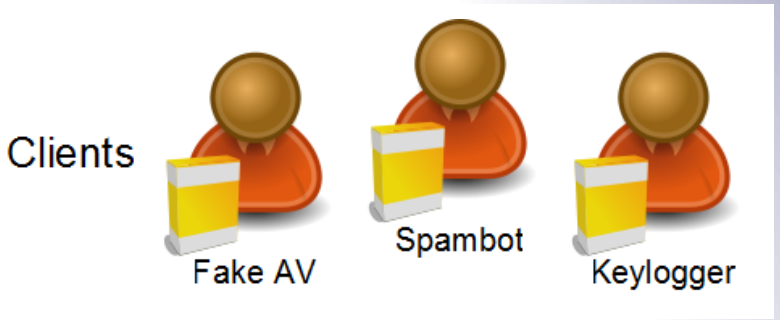
Good or Service	Percent of offerings	Asking price range
Bank account credentials	18%	$10-$1000
Credit Card Numbers (with CCV2)	16%	$0.50-$12
Credit Cards	13%	$0.1-$25
Email addresses	6%	$0.30/MB - $40/MB
Email passwords	6%	$4 - $30
Full identities	6%	$0.90 - $25
Cashout Services	5%	8%-50% of total value
Proxies	4%	$0.30 - $20
Scams	3%	$2.5-$100/week for hosting
Mailers	3%	$1-$25

"Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy," Herley, Florencio

Pay-Per-Install Ecosystem

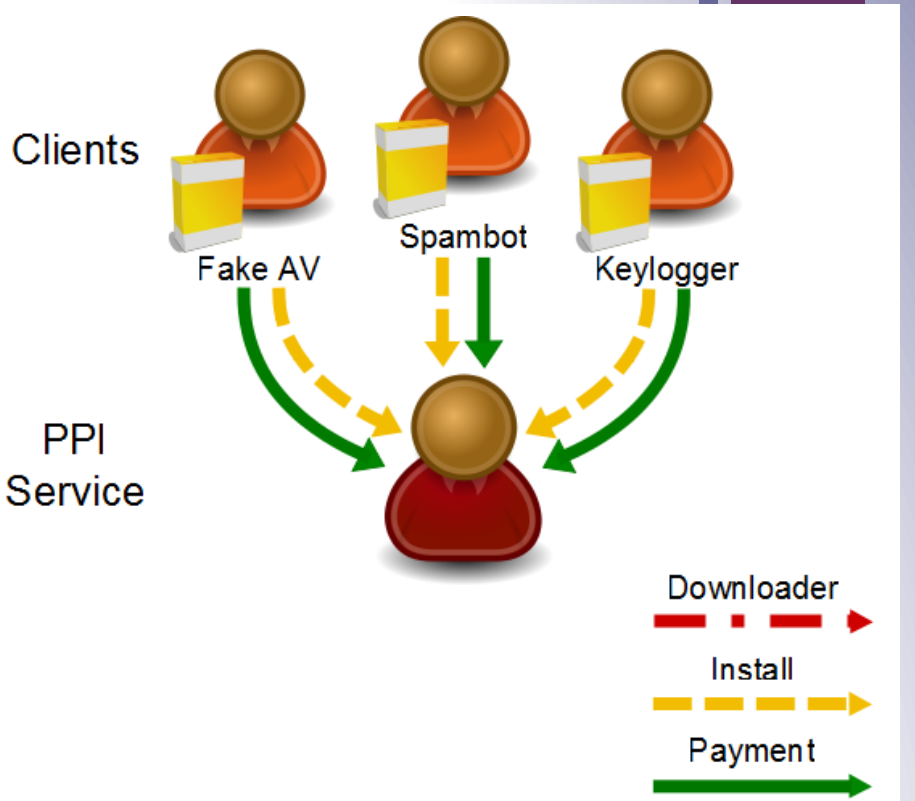
"Measuring Pay-per-Install: The Commoditization of Malware Distribution," Caballero et al.

- Clients
  - Pay the PPI
  - Want malware installed
  - Spambots, information harvesting, rootkits, fake AV



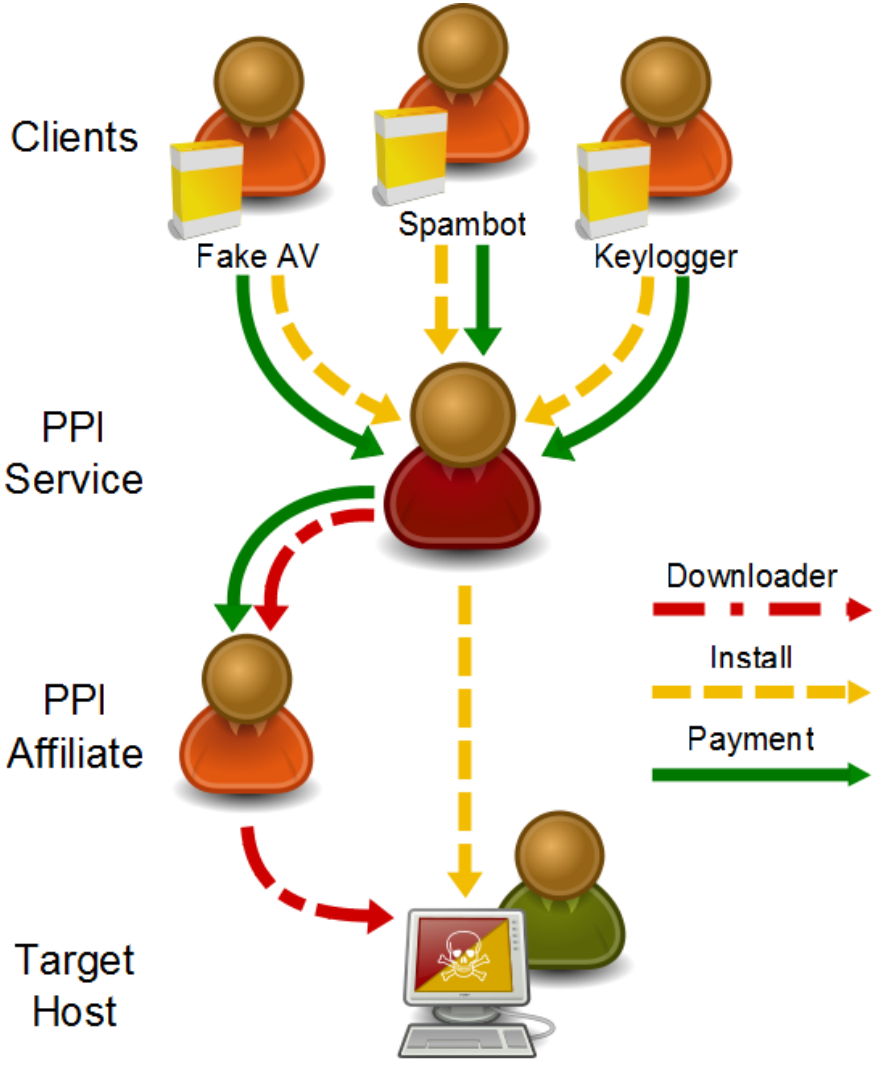
Pay-Per-Install Ecosystem

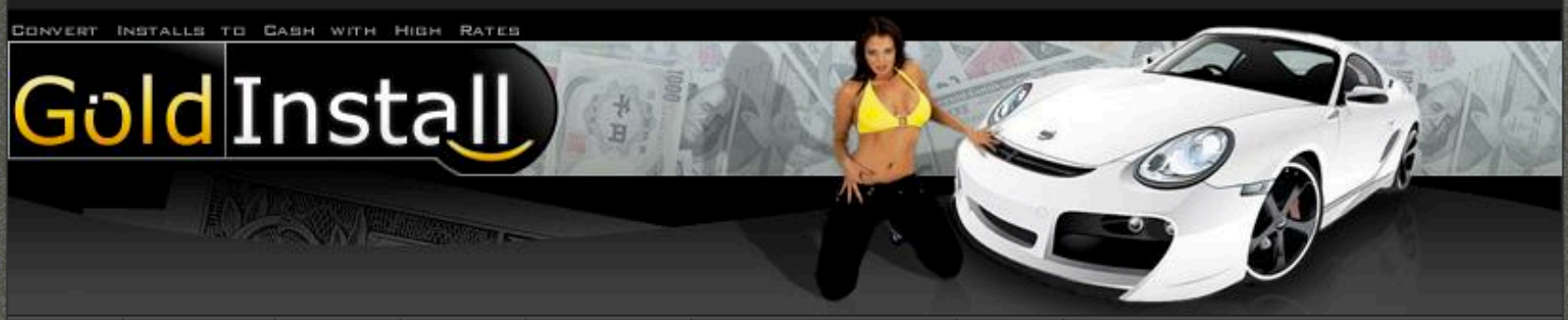
- Clients
  - Pay the PPI
  - Want malware installed
  - Spambots, information harvesting, rootkits, fake AV
- Pay-per-install (PPI)
  - Purchase compromised hosts from affiliates
  - Resells to clients



Pay-Per-Install Ecosystem

- Clients
  - Pay the PPI
  - Want malware installed
  - Spambots, information harvesting, rootkits, fake AV
- Pay-per-install (PPI)
  - Purchase compromised hosts from affiliates
  - Resells to clients
- Affiliates
  - Compromise machines
  - Execute the PPI's binaries





Main | Sign up | Login | Rates | Contacts | Terms of service | FAQ

Prices

Goldinstall Rates for 1K Installs for each Country.

Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$
IT	65$
CH	20$
CZ	20$
DK	20$
ES	30$
AU	55$
FR	30$
NL	20$
NO	20$
PT	30$
LB	6$


Rus | Eng
Gangsta Bucks.com
Statistic
Home
Conditions
Registration
Tariffs
Contacts
An individual approach to everyone
Guaranteed weekly payouts
Round-the-clock support
Detailed statistics
User-friendly software
GangstaBucks.com - it pays on time!
We pay for all installs!
Join our ranks and by tomorrow
you could get your first payout!
Gangsta Bucks

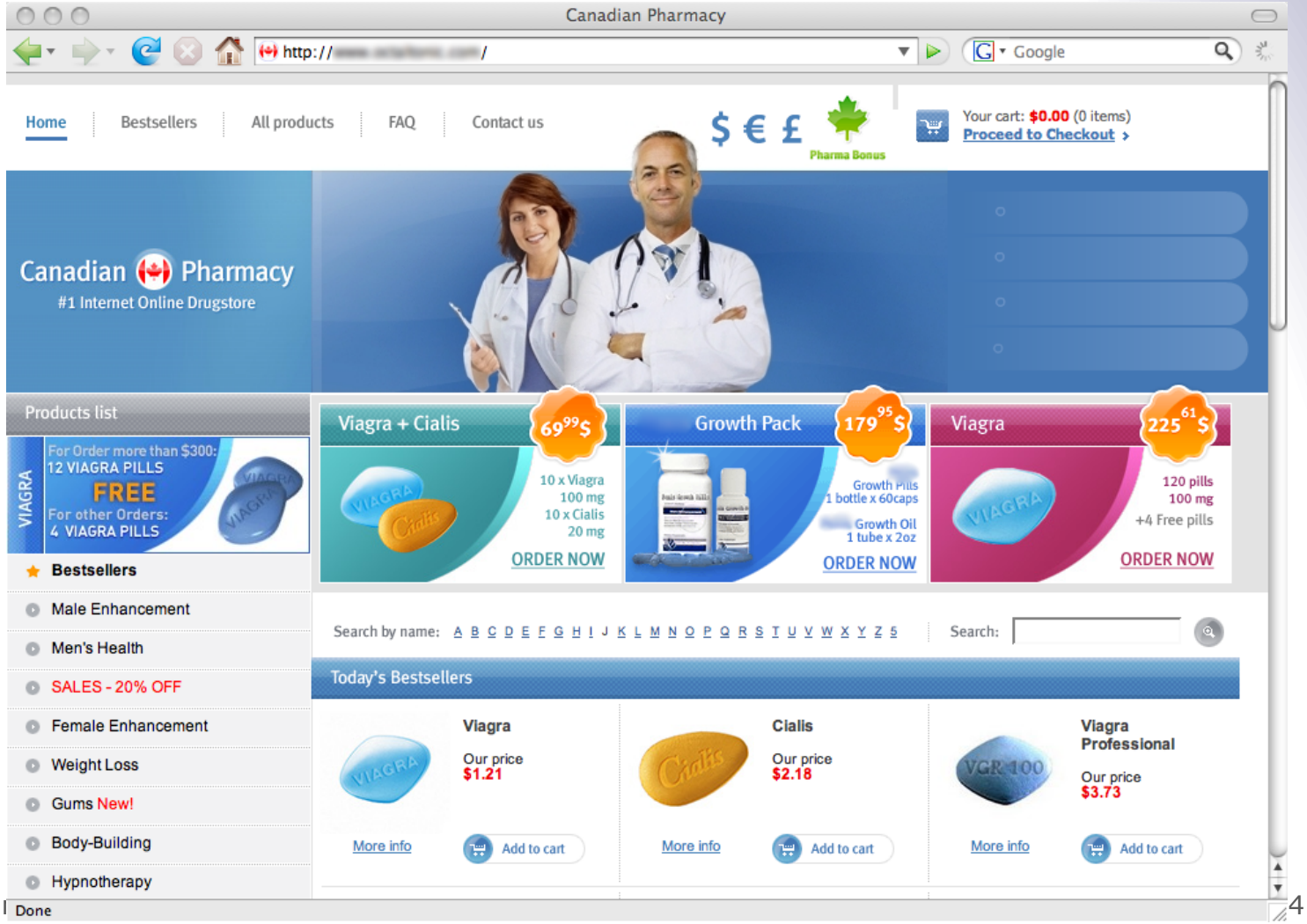
The Underground Economy

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

The Underground Economy

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

Welcome to Storm!
What can we sell you?



Life As A Spammer …

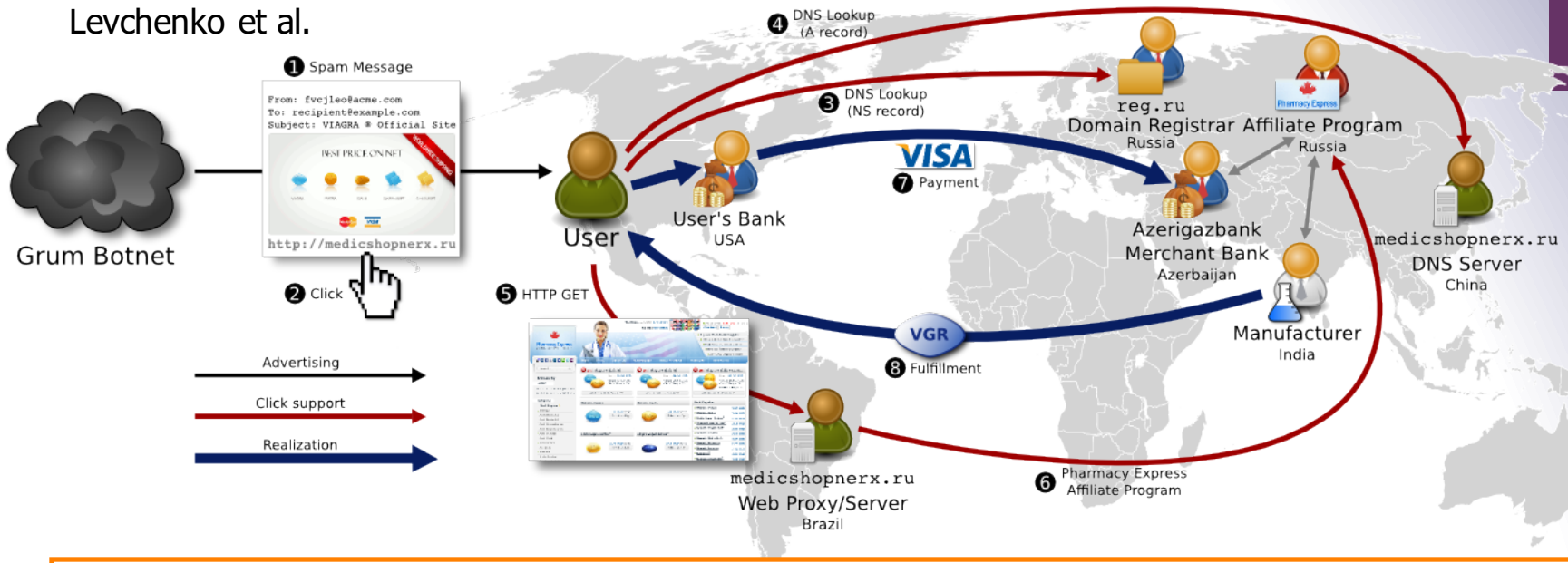
"Spamalytics: An Empirical Analysis of Spam Marketing Conversion," Kanich et al.

- Storm infiltration study found:
  - Modern spam campaigns can send 10s of billions of spams using mailing lists of 100s of millions of addresses
  - 3/4 to 5/6 of all spam delivery attempts fail before the message is even sent to the receiver's server …
    - … due to heavy & effective use of black-listing
  - It takes around 20,000 "postcard" spams to get one person to visit the postcard site
    - 1 in 10 of the visitors will click to download the postcard
  - It takes around 12,000,000 Viagra spams to get one person to visit the site and make a purchase (~$100)
  - Even given those low rates, huge volume ⇒ **profitable**

~ $1.5-2M/year revenue

Phases of the Spam Value Chain

"Click Trajectories: End-to-End Analysis of the Spam Value Chain," Levchenko et al.



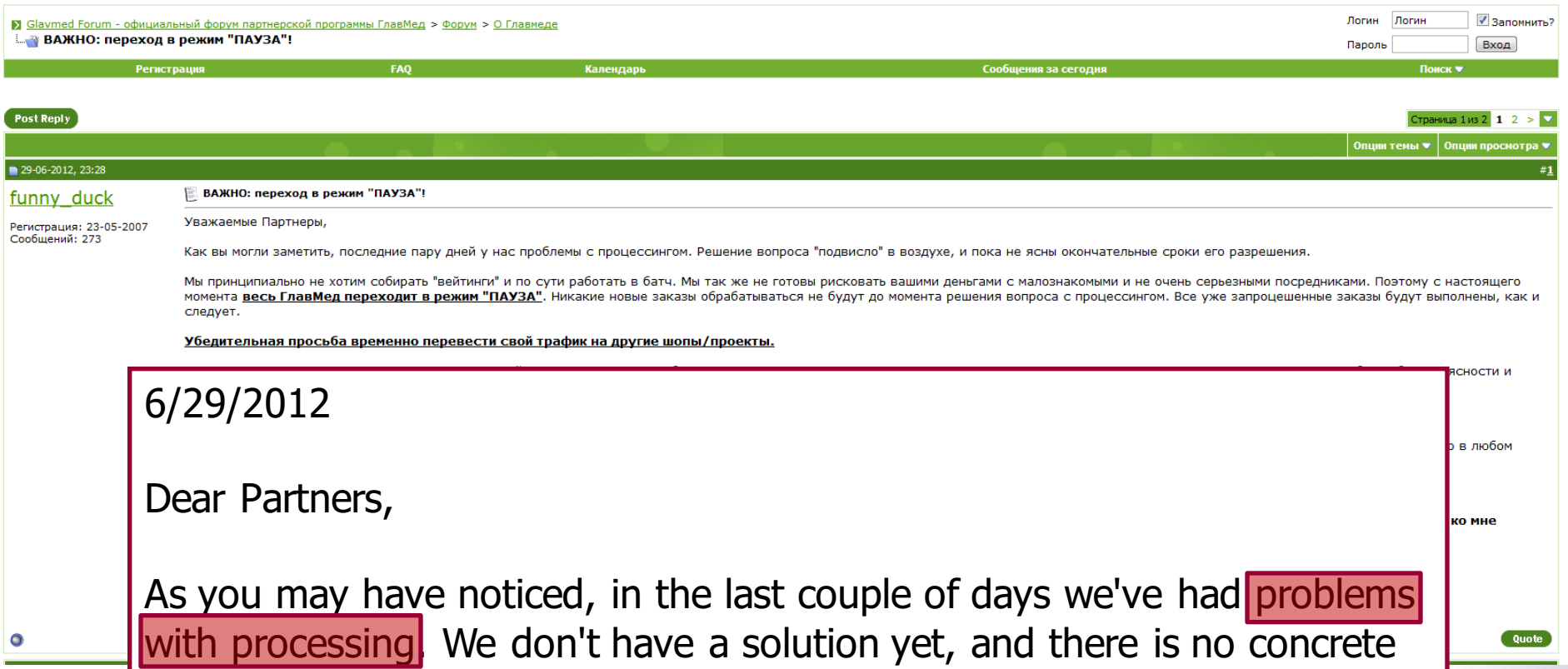
If we were to "snip" a link in this chain, which one would be the most disruptive for our least expenditure?

Measuring URLs, DNS servers, HTTP redirection, etc. all a matter of energetic crawling & recording.

But **merchant banks / Visa / "fulfillment"?**

Harming the Spam Value Chain

- Study based on making purchases of spam-advertised pharmaceuticals found that 3 merchant banks hosted **95+% of all sales** …
- … suggesting a novel way to suppress spam is to undermine the credit-card processing



6/29/2012

Dear Partners,

As you may have noticed, in the last couple of days we've had problems with processing. We don't have a solution yet, and there is no concrete time when it will be resolved.

.....

From this point forward, GlavMed is switching to a "PAUSED" mode. No new orders will be processed until the processing issue is resolved.

.....

We urge you to temporarily switch your traffic to other shops/projects.

Further References

- Symantec Report on the Underground Economy, Symantec, Nov 2008
  - http://bit.ly/1M1xqbS
- Markets for Cybercrime Tools and Stolen Data, RAND, 2014
  - http://bit.ly/1hhycAx
- Spamalytics: An Empirical Analysis of Spam Marketing Conversion, Kanich et al., 2008
  - http://cseweb.ucsd.edu/~klevchen/kklevps-ccs08.pdf
- Measuring Pay-per-Install: The Commoditization of Malware Distribution, Caballero et al., 2011
  - http://bit.ly/1HIxslZ
- Levchenko et al., Click Trajectories: End-to-End Analysis of the Spam Value Chain, 2011
  - http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf

Stay tuned

+

Next time you will learn about

Web Security