# The Underground Economy

*CS 161: Computer Security*

**Prof. Vern Paxson**

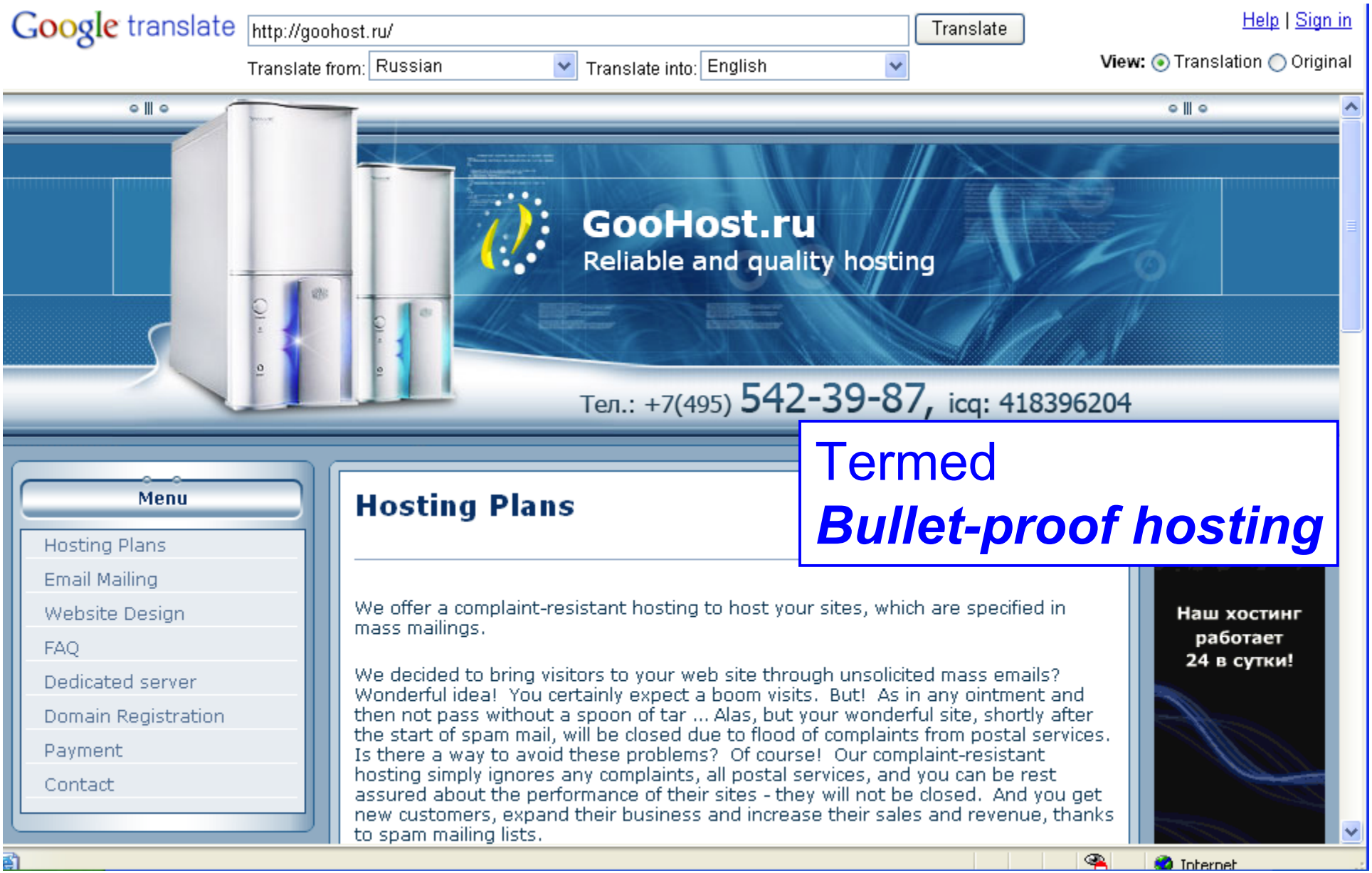
**TAs: Devdatta Akhawe, Mobin Javed & Matthias Vallentin**

*http://inst.eecs.berkeley.edu/~cs161/*

**April 26, 2011**

# Announcements

- Matthias back on May 5
  - Send him email for office hour appointments
- Reminder: Final exam in F295 Haas
  - (**not** Haas Pavilion!)
  - IEEE will provide breakfast munchies
- Course Summary/Review lecture on Thurs
  - TLS, certs, crypto requested by several
  - Possible other topics: DNSSEC, XSS/CSRF
  - … ?


Google translate
http://goohost.ru/
Translate
Translate from: Russian
Translate into: English
Help | Sign in
View: Translation Original
GooHost.ru
Reliable and quality hosting
Тел.: +7(495) 542-39-87, icq: 418396204
Menu
Hosting Plans
Email Mailing
Website Design
FAQ
Dedicated server
Domain Registration
Payment
Contact
Hosting Plans
We offer a complaint-resistant hosting to host your sites, which are specified in mass mailings.
We decided to bring visitors to your web site through unsolicited mass emails? Wonderful idea! You certainly expect a boom visits. But! As in any ointment and then not pass without a spoon of tar ... Alas, but your wonderful site, shortly after the start of spam mail, will be closed due to flood of complaints from postal services. Is there a way to avoid these problems? Of course! Our complaint-resistant hosting simply ignores any complaints, all postal services, and you can be rest assured about the performance of their sites - they will not be closed. And you get new customers, expand their business and increase their sales and revenue, thanks to spam mailing lists.
Termed
Bullet-proof hosting
Наш хостинг работает 24 в сутки!
Internet

**Obuzoustoychivy hosting** is more expensive than usual, but you will have the full guarantee that your site no one ever closes, it will always be available to your customers!

| MINI PLAN | |
|---|---|
| Volume disc | 400 MB |
| Domains | 1 |
| Traffic * | Unlimited |
| FTP-access | there is |
| MySQL database | there is |
| Control panel | there is |
| COST | 4 000 rub. / 1 month. |

| STARTER PLAN | |
|---|---|
| Volume disc | 500 mb |
| Domains | 3 |
| Traffic * | Unlimited |
| FTP-access | there is |
| MySQL database | there is |
| Control panel | there is |
| COST | 5 000 rub. / 1 month. |
| BUSINESS PLAN | |
| Volume disc | 1000 mb |
| Domains | 7 |
| Traffic * | Unlimited |
| FTP-access | there is |
| MySQL database | there is |
| Control panel | there is |
| COST | 7 000 rub. / 1 month. |
| PREMIUM PLAN | |

# Fighting Bots / Botnets, con't

- Approach #2: 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 a 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 … (not yet widely used)
- Counter-counter measure?
  - Behavioral signature: look for hosts that make a lot of failed DNS lookups (research)

# The Problem of Botnets

- Constitute the *Great Modern Threat* of Internet security: *Generic Platform For Badness*
- Why botnets rather than worms?
  - Greater control
  - Less emergent
  - Quieter
  - Optimal flexibility
- Why the shift towards valuing these instead of seismic worm infection events?

  **$$ Profit $$**
- How can attackers monetize botnets?

# Monetizing Botnets

- General malware monetization approaches:
  - Keylogging: steal financial/email/social network accounts
  - Ransomware
  - *Transaction generators*
    - Malware watches user's surfing …
    - … waits for them to log into banking site (say) …
    - … and then injects additional banking transactions like "*send $50,000 to Nigeria*" …
    - … and alters web server replies to mask the change in the user's balance

# Monetizing Botnets, con't

- Monetization that leverages scale
  - DDoS (extortion)
  - Spam
  - *Click fraud*
  - Scam infrastructure
    - Hosting web pages (e.g., phishing)
    - Redirection to evade blacklisting/takedown (DNS)

- Which of these cause serious pain for infected user?
  - **None**. Users have little incentive to prevent (⇒ ***externality***)

Original URL: http://www.theregister.co.uk/2010/03/03/mariposa_botnet_bust_analysis/

# How FBI, police busted massive botnet

## 12m zombie machines run by 3 admins

By **John Leyden**

Posted in Malware, 3rd March 2010 15:56 GMT

**Analysis** More details have emerged about a cybercrime investigation that led to the takedown of a botnet containing 12m zombie PCs and the arrest of three alleged kingpins who built and ran it.

As previously reported, the Mariposa botnet was principally geared towards stealing online login credentials for banks, email services and the like from compromised Windows PCs. The malware infected an estimated 12.7 million computers in more than 190 countries.

The Mariposa Working Group infiltrated the command-and-control structure of Mariposa to monitor the communication channels that relayed information from compromised systems back to the hackers who run the botnet. Analysis of the command system laid the groundwork for the December 2009 shutdown of the botnet, as well as shedding light on how the malware operated and provided a snapshot of the current state of the underground economy.

The botmasters made money by selling parts of the botnet to other cybercrooks,

**Netkairo finally regained control of Mariposa and launched a denial of service attack against Defence Intelligence using all the bots in his control. This attack seriously impacted an ISP, leaving numerous clients without an Internet connection for several hours, including several Canadian universities and government institutions.**

**Once again, the Mariposa Working Group managed to prevent the DDP Team from accessing Mariposa. We changed the DNS records, so the bots could not connect to the C&C servers and receive instructions, and at that moment we saw exactly how many bots were reporting. We were shocked to find that more than 12 million IP addresses were connecting and sending information to the C&C servers, making Mariposa one of the largest botnets in history.**

alleged lieutenants “Ostiator” and “Johnyloleante” have been charged with cybercrime offences. More arrests are expected to follow.

Under Spanish law suspects are not named at this stage of proceedings. Pedro Bustamante, senior research advisor at Panda Security, said: “Our preliminary analysis indicates that the botmasters did not have advanced hacking skills.

"This is very alarming because it proves how sophisticated and effective malware distribution software has become, empowering relatively unskilled cyber criminals to inflict major damage and financial loss." ®

# Spy Instructors Software

NEW GENERATION SOFTWARE SOLUTIONS

HOMEPAGE | PRODUCTS | DOWNLOADS | FORUMS | ABOUT US

## ProAgent v2.1

- ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.
- It is an ultimate solution for monitoring spouses, children, employees, or anyone else!
- ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!
- ProAgent can work in all kind of networks, it doesn't matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase **ProAgent v2.1** Special Edition...

Click here to download **ProAgent v2.1** Public Edition

## SIS - Products

Purchase Program

Customer Support Department

Commercial Programs

Freeware Programs

Custom Special Programs

New Generation Software Solutions...

## New Products

**SIS-IExploiter v2.0**


**ProAgent v2.1**


**AntiDote v1.2**

**SIS-Downloader**

**Virtual Keyboard**


# Список доступных акков

**Сервис по продаже аккаунтов аукцыона eBay.**

Добрые юзеры аукцыона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
**Все** аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субьективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гарант сервис приветствуется.

**Мои цены:**

**seller/баер акк до 10 фидов = 5$**
**seller/баер акк 10-25 фидов = 10$**
**seller/баер акк 25-50 фидов = 15$**
**seller/баер акк более 50 фидов = 25$**

# allBots Inc.

## Social Networking Bots

**GOOD News!!!** We have something more for you! Yes, we have just integrated **CAPTCHA Bypasser**** in all of our bots.

**Winsock (Multi-threaded) Bots**

**Become an Affiliate and Start Earning Now**

**Click here for 30+ MySpace Bots**

## Accounts Creator

(You Just Need To Type In The CAPTCHAs To Create Accounts)

| Social Networks | | | |
|---|---|---|---|
| MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager | PayPal Buy Now | ~~$180.95~~ | $140.00 |
| MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock) | PayPal Buy Now | ~~$360.95~~ | $320.00 |
| YouTube Accounts Creator | PayPal Buy Now | ~~$120.95~~ | $95.00 |
| Friendster Accounts Creator | PayPal Buy Now | ~~$120.95~~ | $95.00 |
| Hi5 Accounts Creator | PayPal Buy Now | ~~$120.95~~ | $95.00 |
| TagWorld Accounts Creator | PayPal | | |

## Friend Adders, Message Senders, Comment Posters & Others

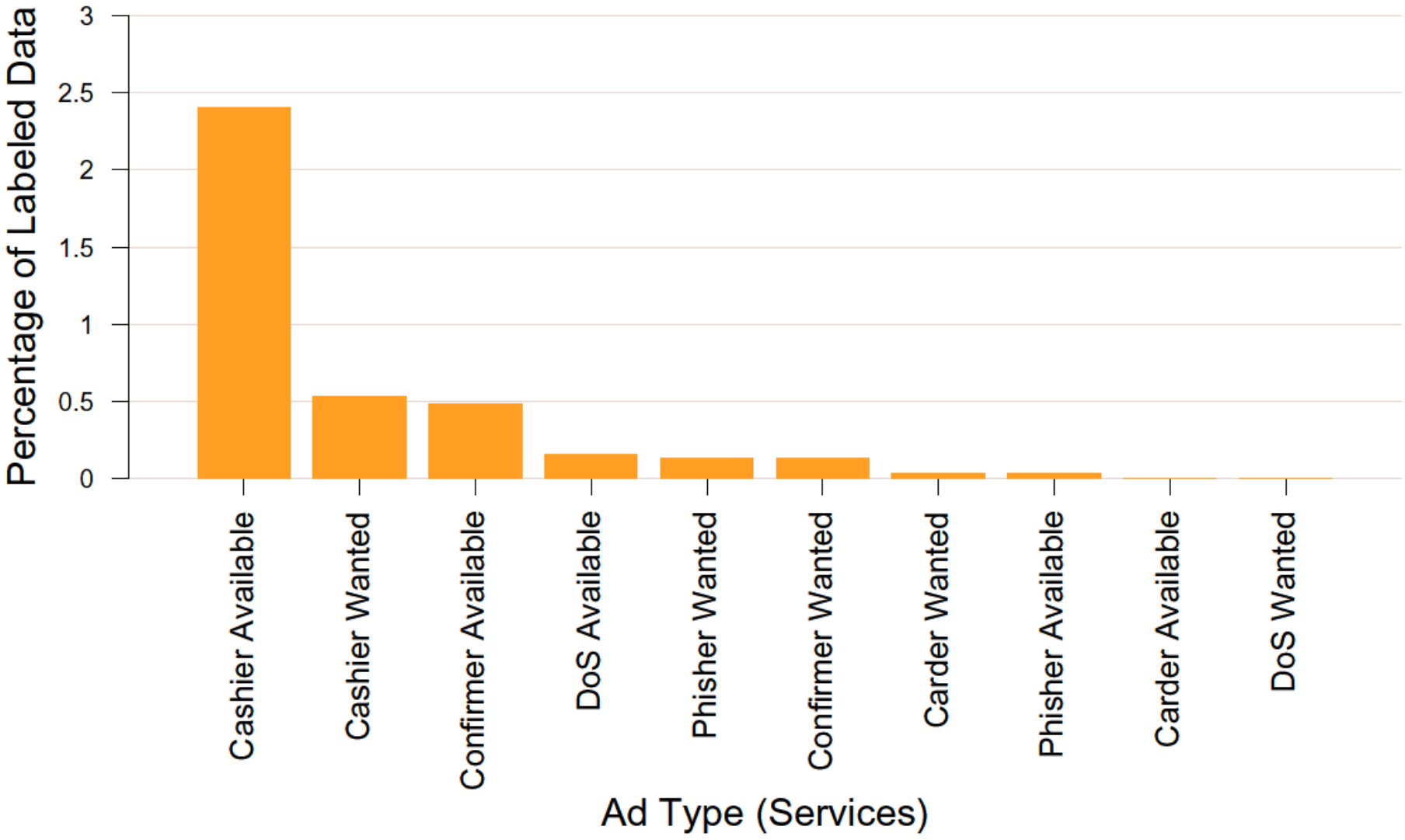
(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)

**Chaining Feature** Is Available On All Bots for All Networks Except Facebook

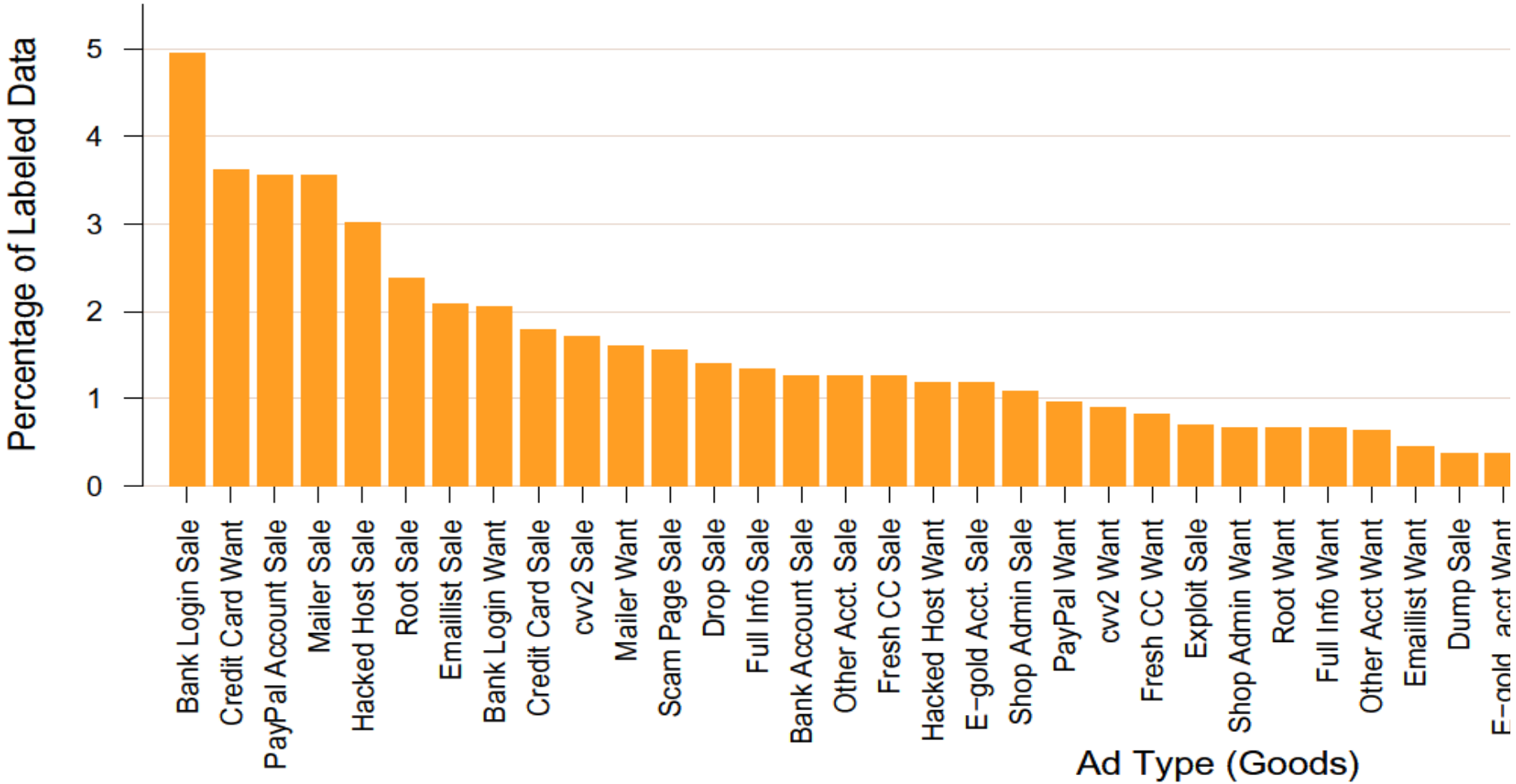
**Advertisement**

i have boa wells and barclays bank logins....
have hacked hosts, mail lists, php mailer send to all inbox
i need 1 mastercard i give 1 linux hacked root
i have verified paypal accounts with good balance...and i can cashout paypals

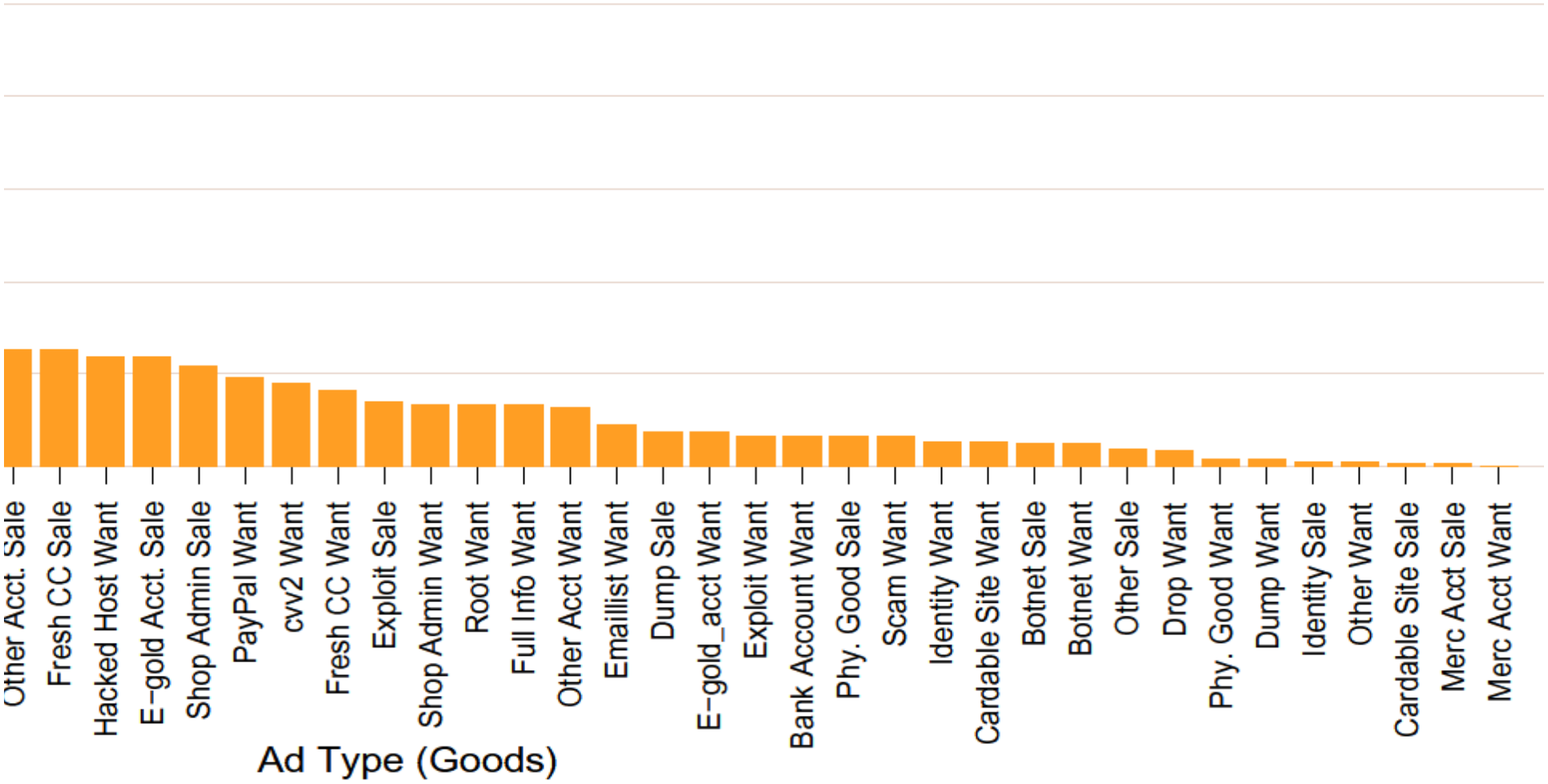
# Marketplace Ads for Services



# Marketplace Ads for Goods



# Marketplace Ads for Goods, con't



# The Underground Economy

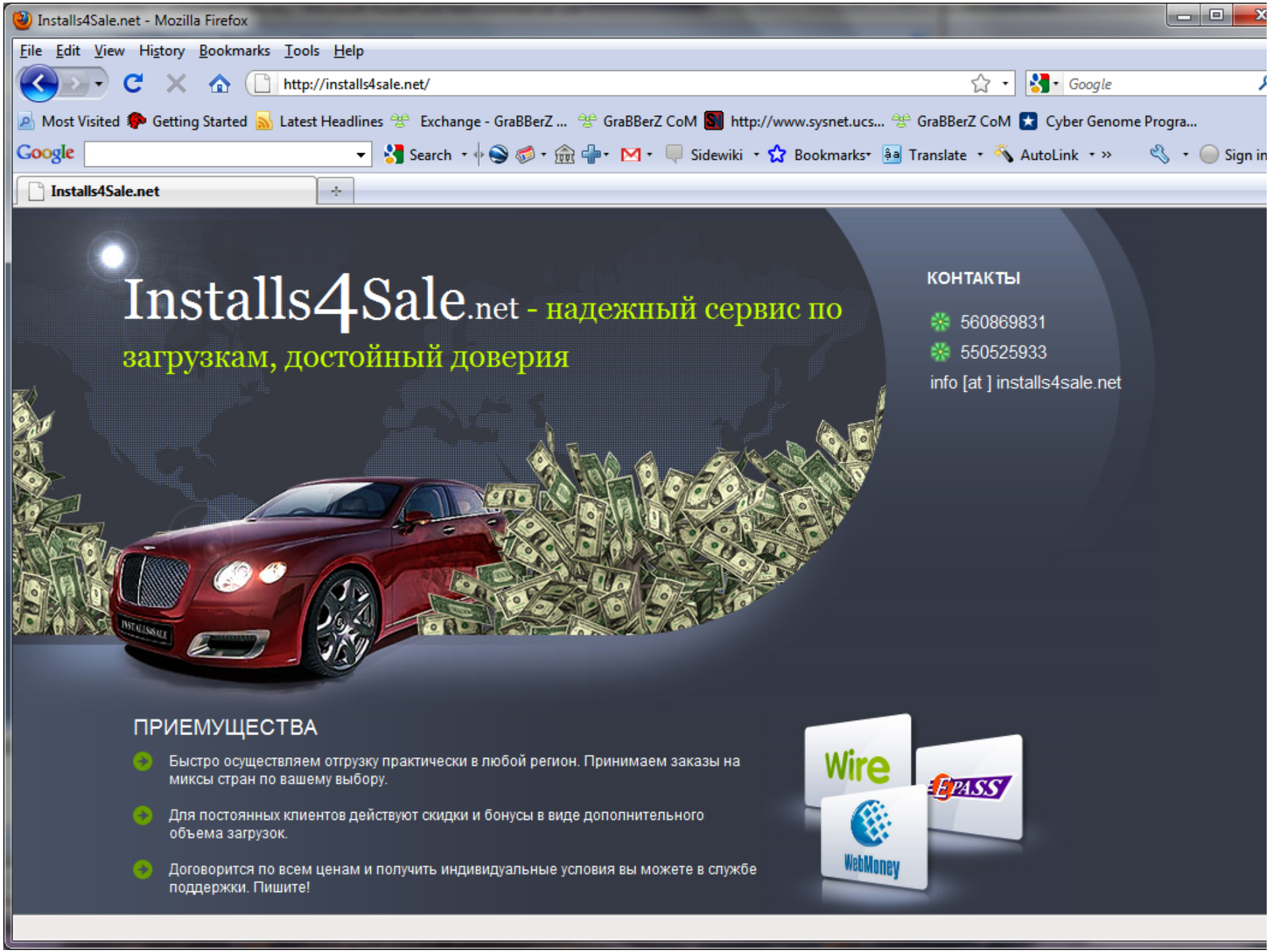
- Why is its emergence significant?

- 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, con't

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

# Pay-Per-Install (PPI)


Installs4Sale.net - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://installs4sale.net/
Google
Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Progra...
Search Sidewiki Bookmarks Translate AutoLink Sign in
Installs4Sale.net
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия
КОНТАКТЫ
560869831
550525933
info [at ] installs4sale.net
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.
Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
Wire
EPASS
WebMoney

CONVERT INSTALLS TO CASH WITH HIGH RATES

GoldInstall

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$ |

Earning4u.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://earning4u.com/index.php?l=en

Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Pr

Google "underground economy" blackhat Search Sidewiki Bookmarks Translate

Earning4u.com

EARNING 4-U .COM

ENTER STATS

BETTER RATES! NO HOLD!
ONLY REAL ONLINE STATISTIC!

REGISTER TODAY

MAIN | ABOUT US | CONDITIONS | RATES | FAQ | CONTACTS

**The partnership program «Earning4u»** is the easiest way to earn money.
All you need to do to start working with us is register.

You will earn **from 6$**(Asia) **to 180$**(USA) per 1000 installs. You can view all prices in the «Rates» section.

## Key **Features**

Thanks to an individual approach to each client when you work with our system you have:

- Online statistics updated in real time
- A 24-hour support service ready to answer all your questions
- Absolutely no shaving and total independence of your statistics from other system users
- Stable weekly payments on virtually all payment systems: Fethard, WebMoney, Wire, e-gold, Western Union (WU), MoneyGram, Anelik and ePassporte, and PayPal

Best Pay-Per-Install affiliate program reviews. ActiveX affiliates. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.pay-per-install.com/ Go Links

PAY PER INSTALL AFFILIATE PROGRAMS

Today is: Tuesday 16. November 2010

CLICK HERE TO VISIT OUR BEST SPONSOR.

WE WORK
Even when you sleep!

One of the best PPI programs. Up to $180 per 1000 Installs.

**Affiliate Program NewsLetter** Get new programs via email

Insert your Email Address: Subscribe

**JOIN MAKE MONEY FORUM**

Learn How to make money with PPN Gateway

Free guide to teach you how to make $7000 per day

# Best Pay-Per-Install affiliate program reviews. ActiveX affiliates.

BOOKMARK US

MAKE MONEY CATEGORIES
- Pay Per Click
- Pay Per Impression
- Bid Search Engines
- Pay Per Lead
- Pay Per Install

OTHERS
- CONTACT

GET PAID from each toolbar install

Best Pay-per-install affiliate programs on the net. Earn money with any traffic, these ActiveX affiliates will convert anything and make you rich. Payments are up to $1.50 per install. You usualy distribute installation of toolbar and making cash. You can also make loads of money with content sites such are movies, games, mp3 and protect your content with Content Gateways which are paying most, to unlock the content user needs to install simple adware application and than he can get content for free.

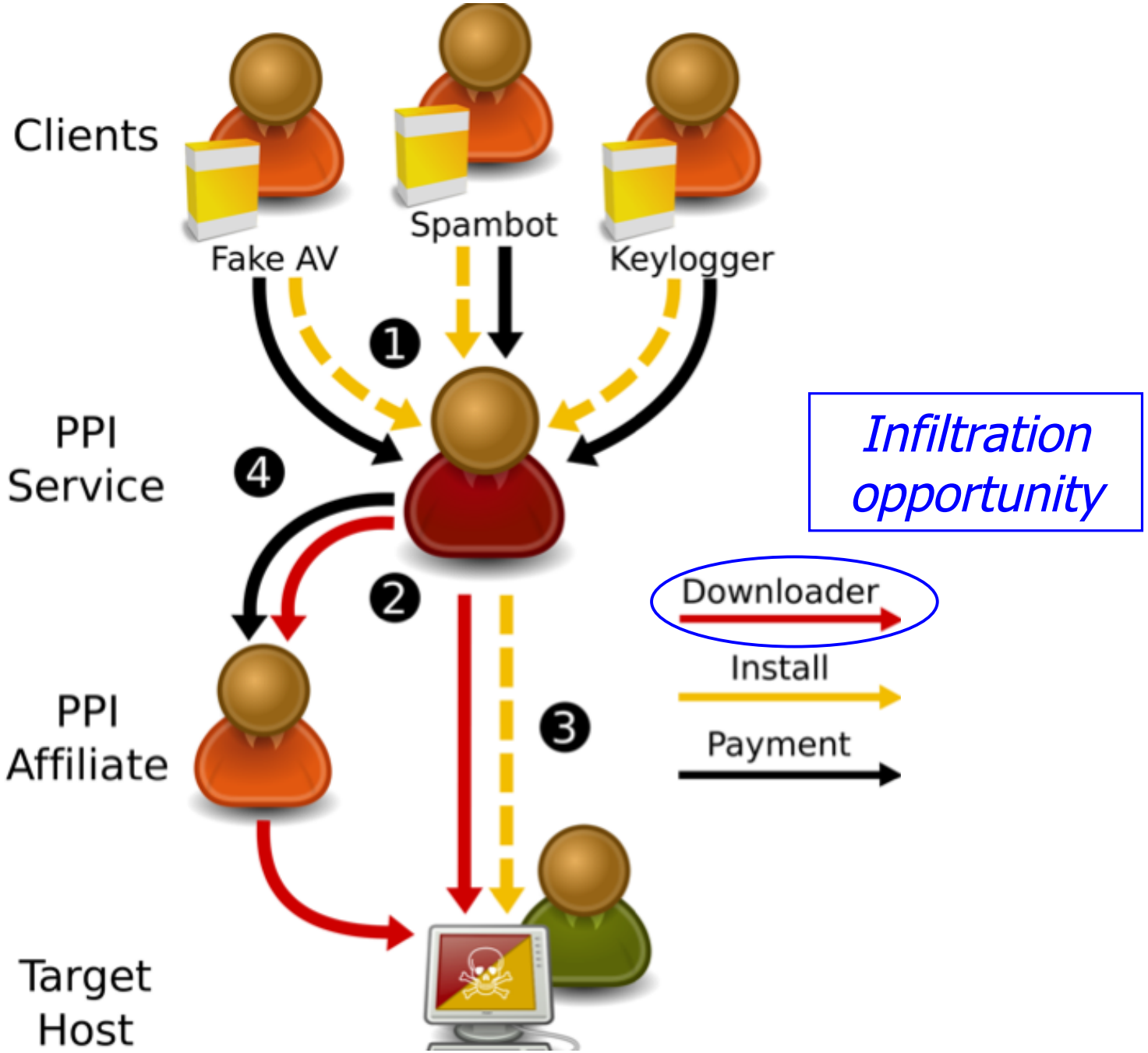
All Pages: [0] [1] [2] [3] [4]

**Make money with these BEST AFFILIATE PROGRAMS**

Rank Sponsors

BOOKMARK US

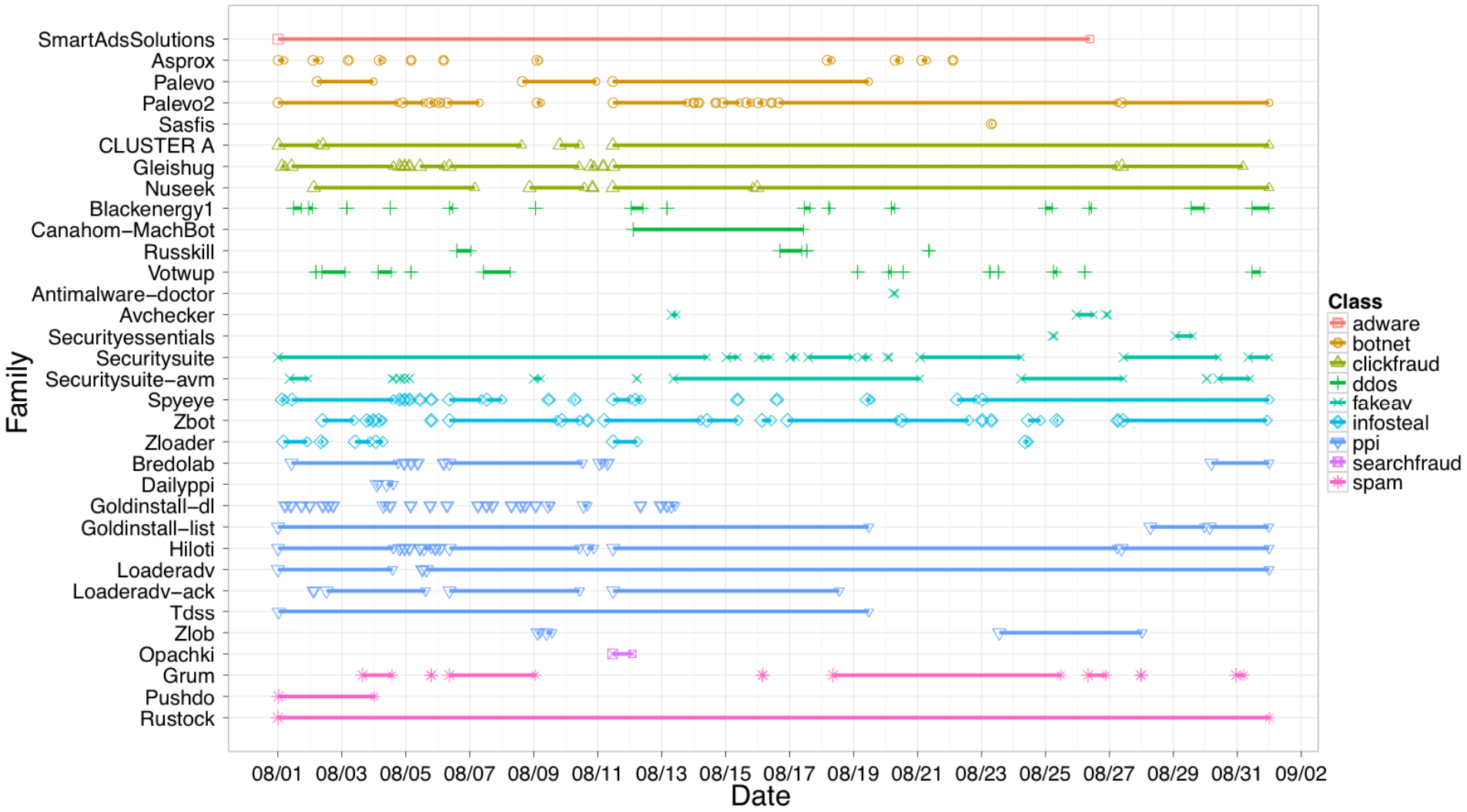
Last 10 Reviews
- CPALead - November/13/2010
- SexSearch - October/31/2010
- LoudMo - October/28/2010
- SexSearch - October/18/2010
- SexSearch - October/18/2010
- ioXes - October/12/2010
- Earning4u - September/09/2010
- Earning4u - August/30/2010


Clients
Fake AV
Spambot
Keylogger
1
PPI
Service
4
2
3
PPI
Affiliate
Target
Host
Infiltration
opportunity
Downloader
Install
Payment

| | NAME | % | MONETIZATION | KIT | SEEN |
|---|---|---|---|---|---|
| 1 | Palevo | 7.50 | DoS,Info stealer | ✓ | ✓ |
| 2 | Hiloti | 4.69 | Downloader/PPI | | ✓ |
| 3 | Zbot | 3.62 | Info stealer | ✓ | ✓ |
| 4 | FakeRean | 3.47 | Rogue AV(s) | | ✓ |
| 5 | Onlinegames | 2.94 | Info stealer | | ? |
| 6 | Rustock | 2.66 | Spam | | ✓ |
| 7 | Ldpinch | 2.64 | Info stealer | ✓ | ? |
| 8 | Renos | 2.58 | Rogue AV(s) | | ? |
| 9 | Zlob | 2.54 | Rogue software | | ✓ |
| 10 | Autoit | 2.53 | Downloader/PPI | | |
| 11 | Conficker | 2.48 | Worm | | |
| 12 | Opachki | 1.95 | Click Fraud | | ✓ |
| 13 | Buzus | 1.91 | Info stealer | | |
| 14 | Koobface | 1.17 | Downloader | | |
| 15 | Alureon | 1.16 | Downloader | ✓ | ✓ |
| 16 | Bredolab | 1.15 | Downloader/PPI | ✓ | ✓ |
| 17 | Piptea | 1.13 | Downloader/PPI | | ✓ |
| 18 | Ertfor | 0.91 | Rogue AV(s) | | ✓ |
| 19 | Virut | 0.91 | Downloader/PPI | | ✓ |
| 20 | Storm 2.0 | 0.80 | Spam | | |

Table 2: FireEye's top 20 malware families observed in their MAX Cloud network on the April–June 2010 time

The majority of the world's top malware appeared in PPI downloads




PPI distribution of malware during August 2010

# Spam & Spam Profit

# Modern Spam Operations

- To make the issues concrete, let's take a tour of a modern "spambot"
  = Botnet primarily used for sending spam

- Goal is to get a sense of:
  - Botnet construction
  - Email spam-sending process
  - Arms-race issues

- Note: not comprehensive
  - E.g., there's also blog spam, social network spam, etc.

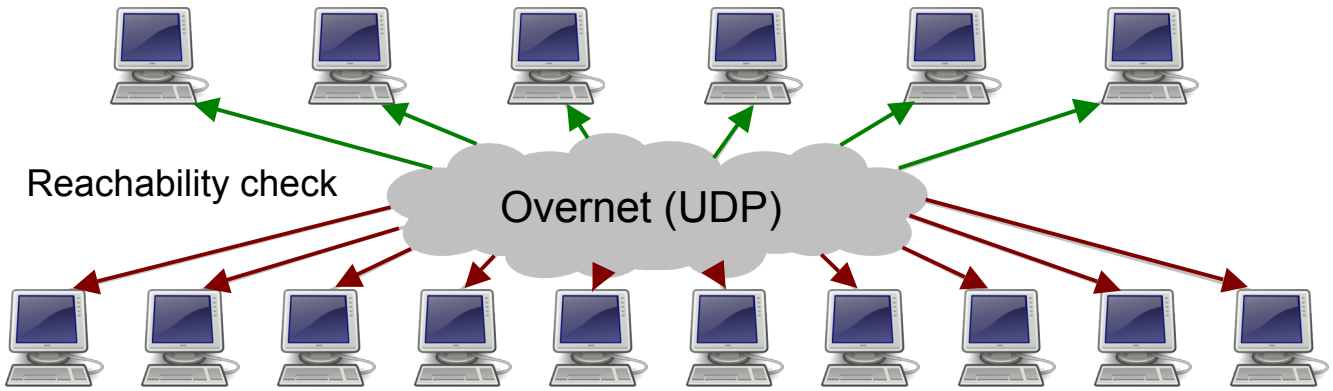
# Welcome to **Storm**!


Would you like to be one of our newest bots?

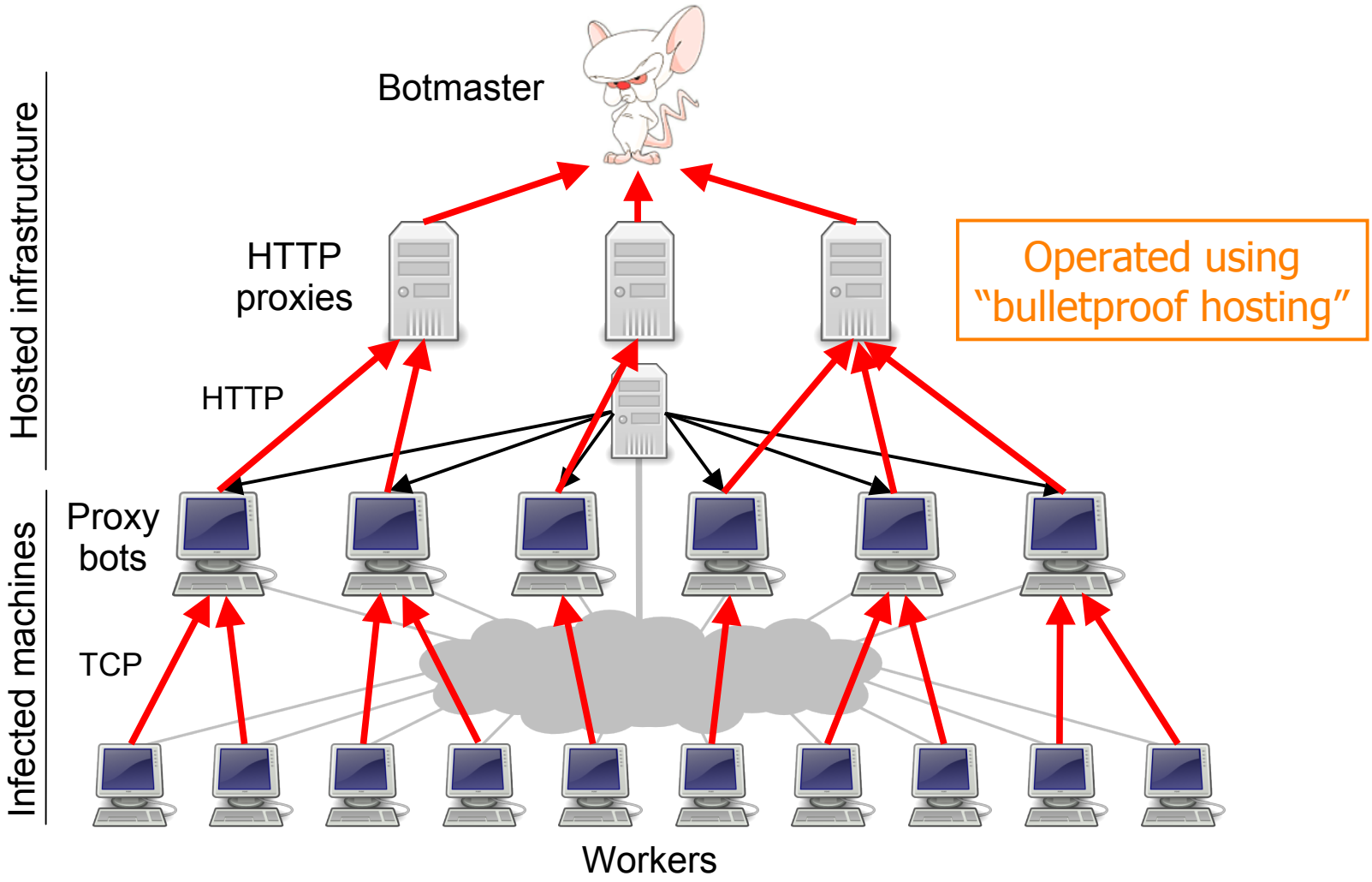
Just read your postcard!

(Or even easier: just wait 5 seconds!)

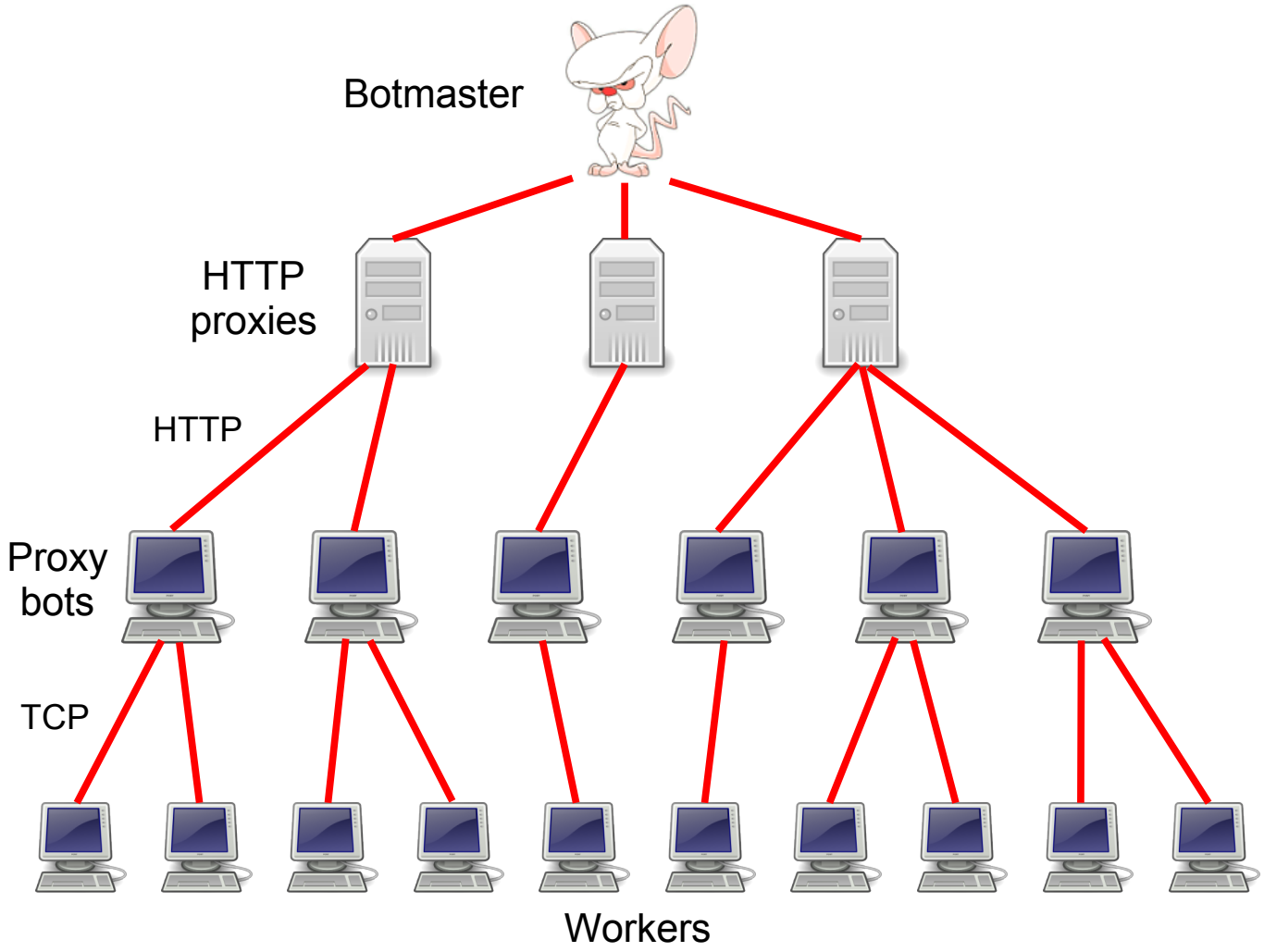
# The *Storm* Botnet



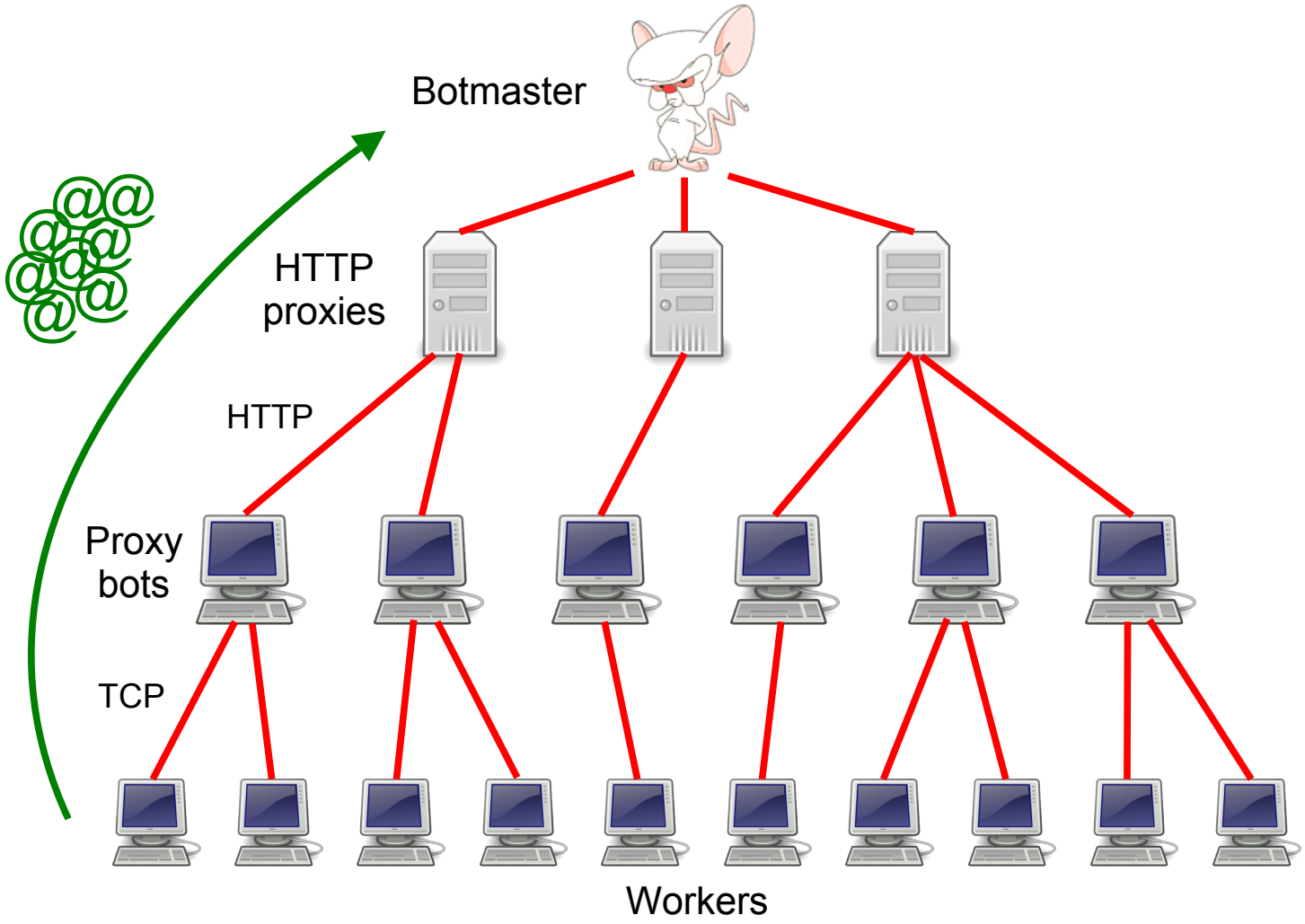
# The *Storm* Botnet



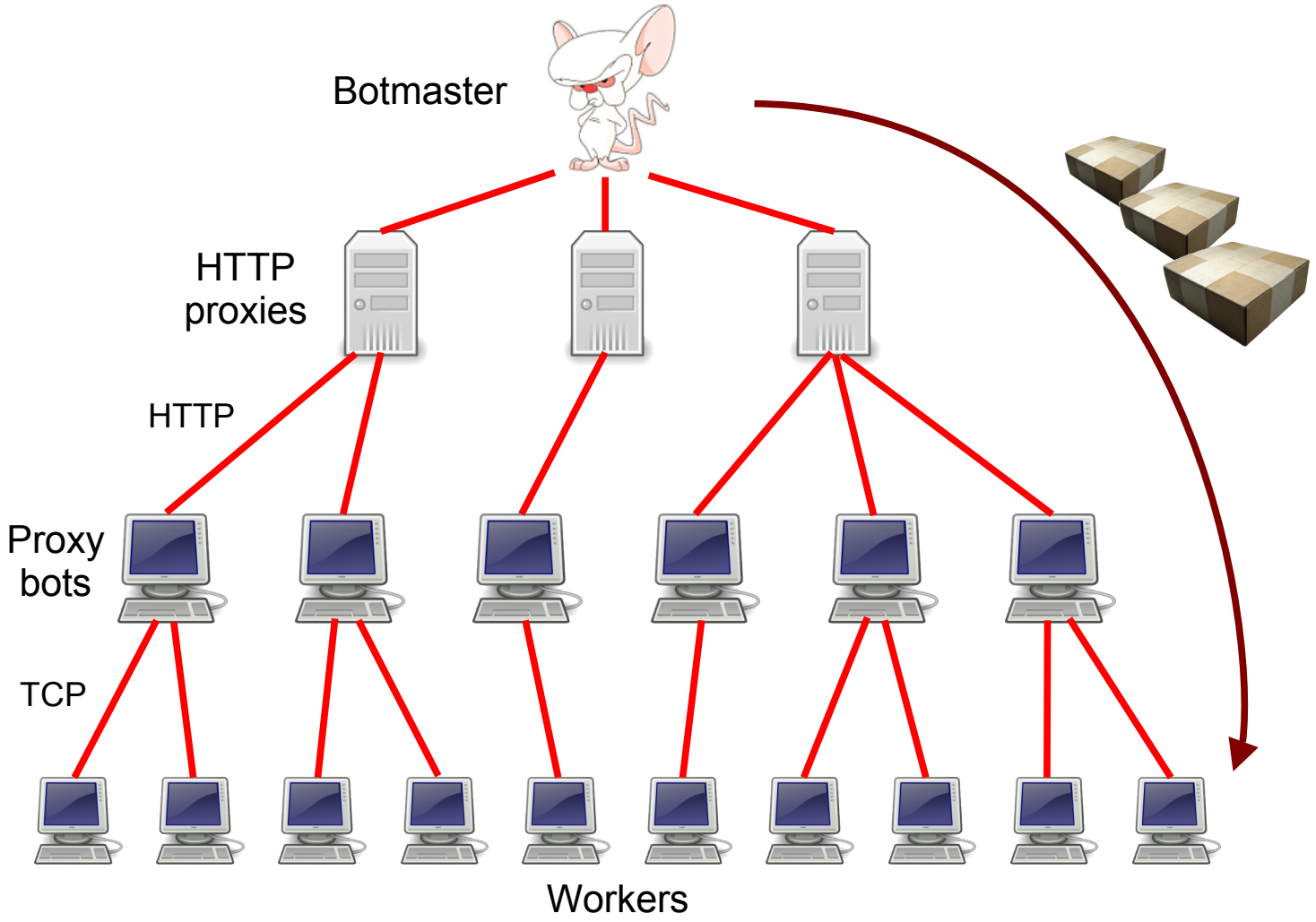
# Spam “Campaign” Mechanics



# Campaign Mechanics: Harvest



# Campaign Mechanics: Spamming



```
Received: from %^C0%^P%^R2-6^%:qwertyuiopasdfghjklzxcvbnm^%.%^P%^R2-6^%:qwertyuiopasdfghjkl ▷
                                                zxcvbnm^%^% ([%^C6%^I^%.%^I^%.%^I^%.%^I^%^%]) by ▷
                                                %^A^% with Microsoft SMTPSVC(%^Fsvcver^%); %^D^%
Message-ID: <%^O%^V6^%:%^R3-50^%^%%^V0^%>
From: <%^Fnames^%@%^Fdomains^%>
To: <%^0^%>
Subject: JOB $1800/WEEK - CANADIANS WANTED!
Date: %^D-%^R30-600^%^%
```

---

```
Received: from auz.xwzww ([132.233.197.74]) by dsl-189-188-79-63.prod-infinitum.com.mx with ▷
                          Microsoft SMTPSVC(5.0.2195.6713); Wed, 6 Feb 2008 16:33:44 -0800
Message-ID: <002e01c86921$18919350$4ac5e984@auz.xwzww>
From: <katiera@experimentalist.org>
To: <voelker@cs.ucsd.edu>
Subject: JOB $1800/WEEK - CANADIANS WANTED!
Date: Wed, 6 Feb 2008 16:33:44 -0800
```

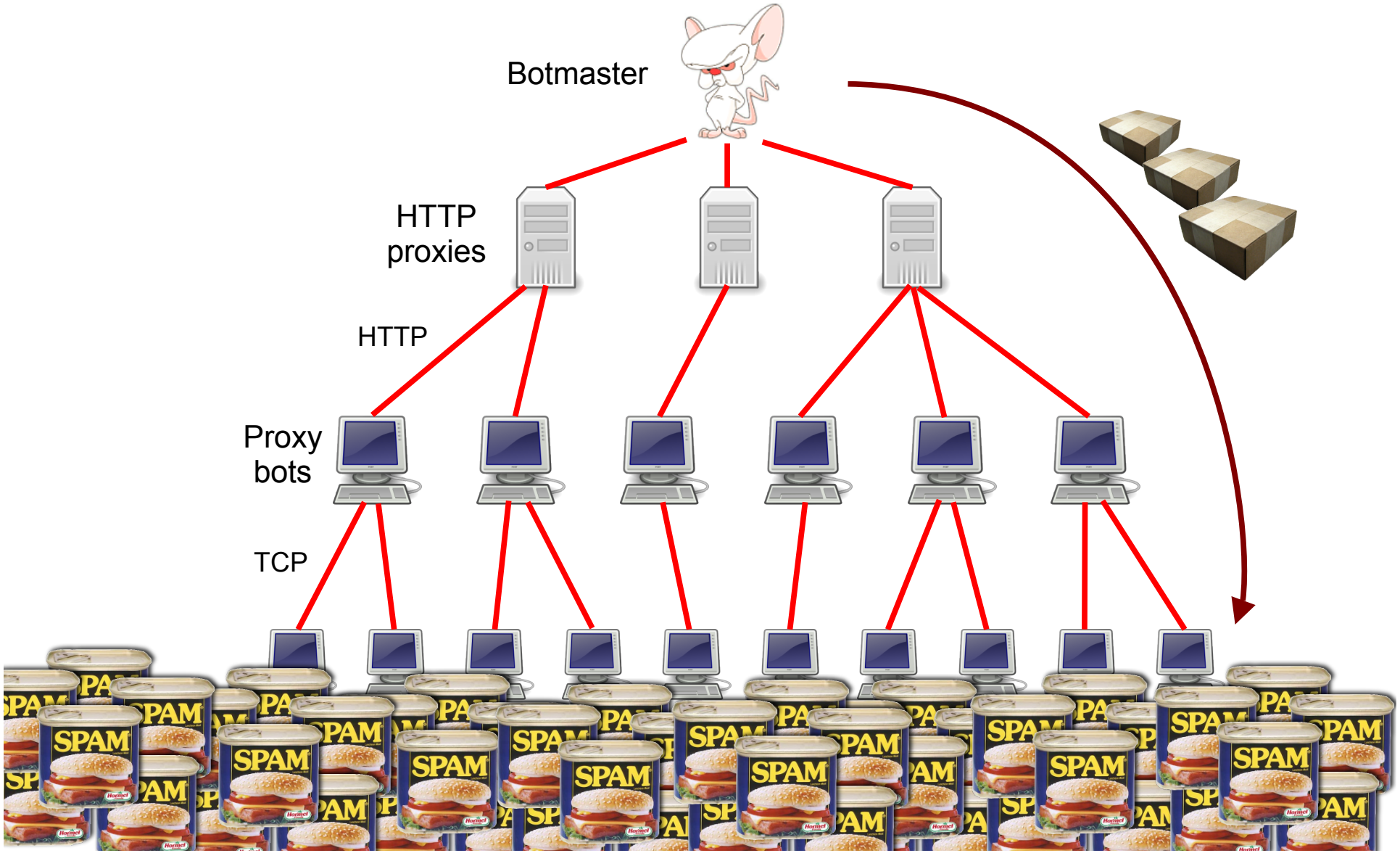
Figure 2: Snippet of a spam template, showing the transformation of an email header from template (top) to resulting content (bottom). The ▷-symbol indicates line continuations. Bold text corresponds to the formatting macros and their evaluation.

Synthetic diversity aims to thwart content-based anti-spam filtering

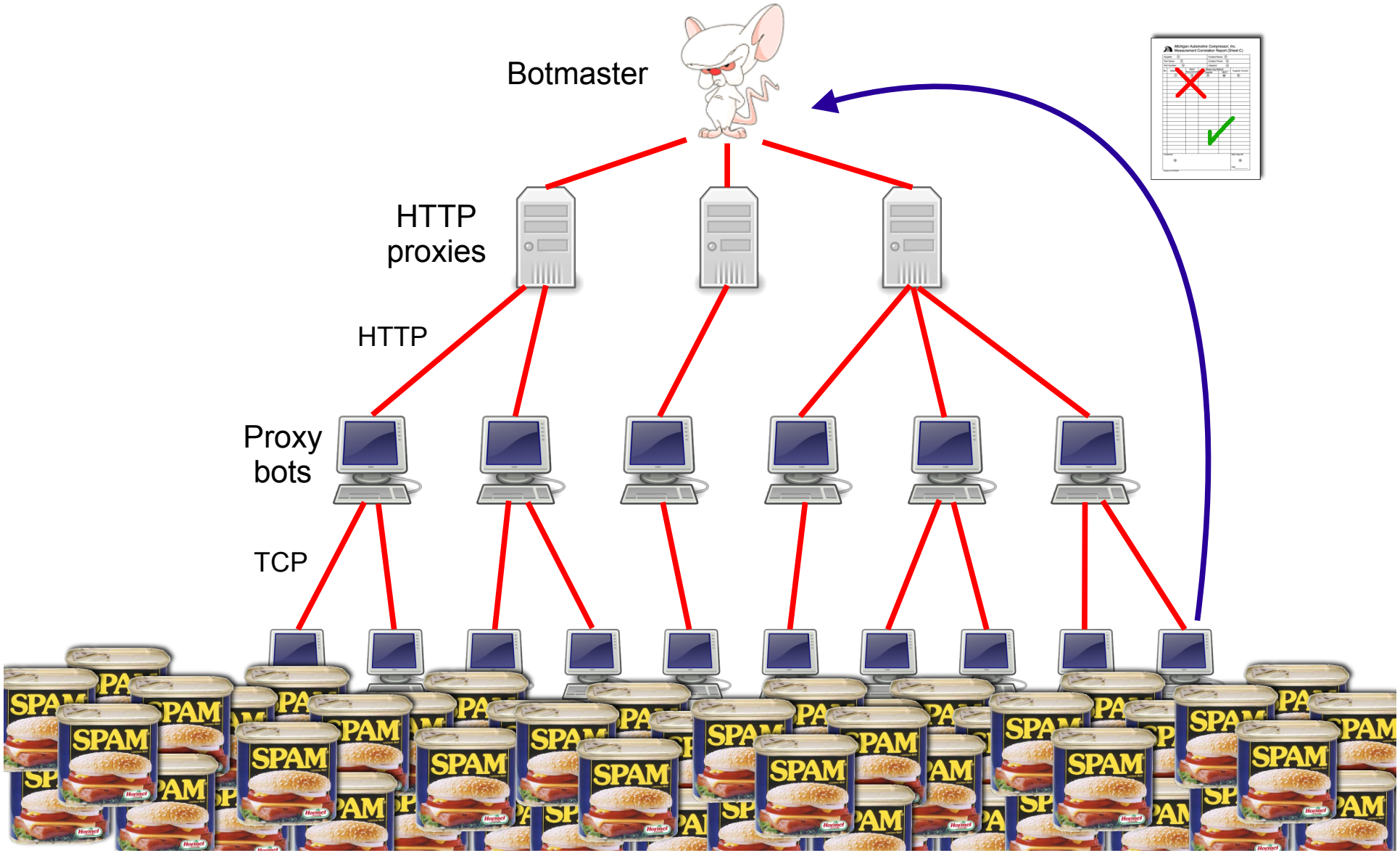
| MACRO | SEEN LIVE | FUNCTIONALITY |
|---|---|---|
| (0) | ✓ | Spam target email address. |
| (A) | ✓ | FQDN of sending bot, as reported to the bot as part of the preceding C&C exchange. |
| (B) | | Creates content-boundary strings for multi-part messages. |
| (C*num*) | ✓ | Labels a field's resulting content, so it can be used elsewhere through (V); see below. |
| (D) | ✓ | Date and time, formatted per RFC 2822. |
| (E) | | ROT-3–encodes the target email address. |
| (F*string*) | ✓ | Random value from the dictionary named *string*.[2] |
| (G*string*) | ✓ | Line-wrap *string* into 72 characters per line. |
| (H*string*) | | Defines hidden text snippets with substitutions, for use in HTML- and plain-text parts. |
| (I) | ✓ | Random number between 1 and 255, used to generate fake IP addresses. |
| (J*string*) | | Produces quoted-printable "=20" linewrapping. |
| (K) | | IP address of SMTP client. |
| (M) | ✓ | 6-character string compatible with Exim's message identifiers (keyed on time). |
| (N) | | 16-bit prefix of SMTP client's IP address. |
| (O*string*:*num*) | ✓ | Randomized message identifier element compatible with Microsoft SMTPSVC. |
| (P$num_1$[-$num_2$]:*string*) | ✓ | Random string of $num_1$ (up to $num_2$, if provided) characters taken from *string*. |
| (Q*string*) | | Quoted-printable "=" linewrapping. |
| (R$num_1$-$num_2$) | ✓ | Random number between $num_1$ and $num_2$. Note, special-cased when used with (D). |
| (U*string*) | | Randomized percent-encoding of *string*. |
| (V*num*) | ✓ | Inserts the value of the field identified by (C*num*). |
| (W) | | Time and date as plain numbers, e.g. "20080225190434". |
| (X) | | Previously selected member of the "names" dictionary. |
| (Y*num*) | ✓ | 8-character alphanumeric string, compatible with Sendmail message identifiers. |
| (Z) | ✓ | Another Sendmail-compatible generator for message identifiers. |

Table 2: Storm's spam-generation templating language.

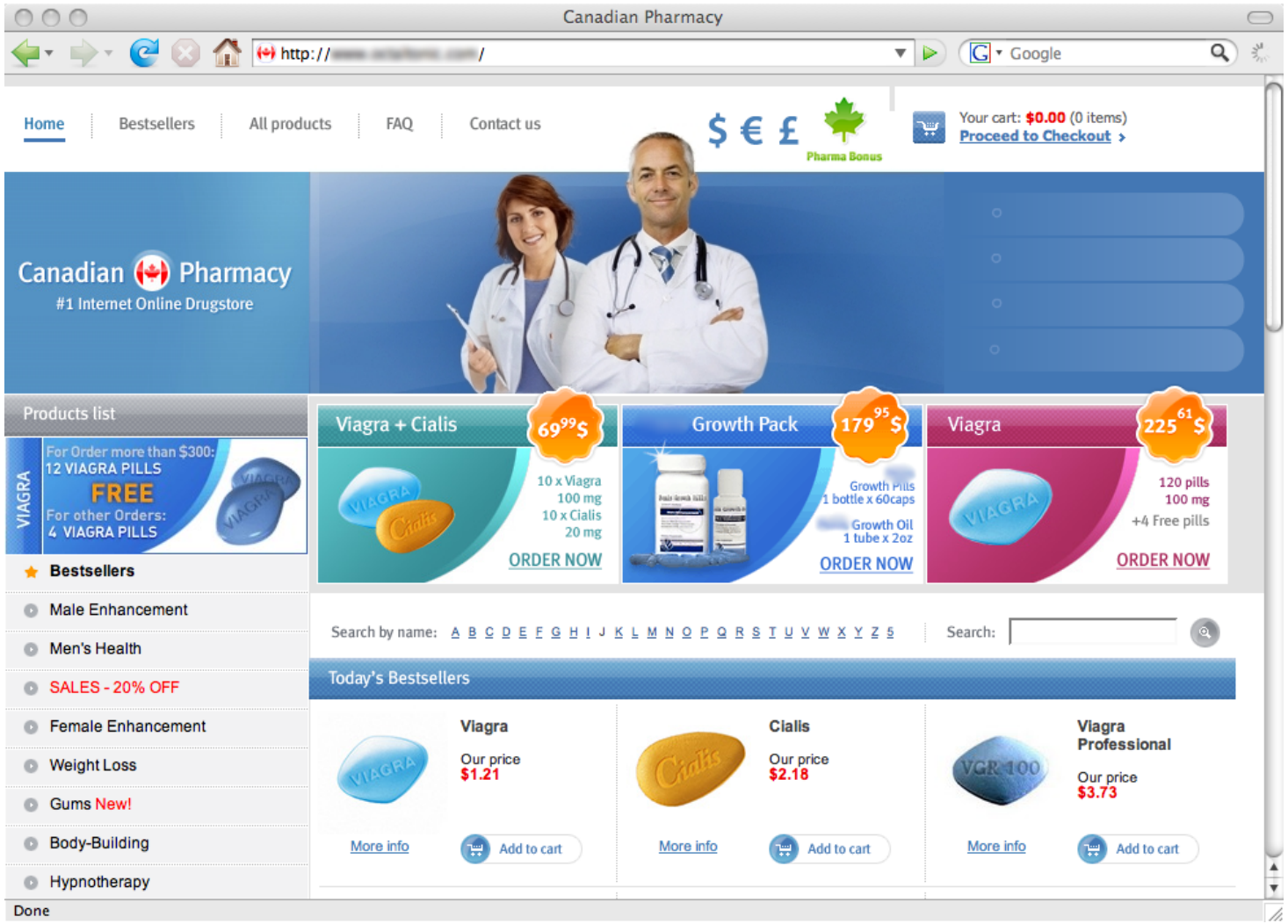
# Campaign Mechanics: Spamming



# Campaign Mechanics: Reporting



# Welcome to **Storm**!  What can we sell you?



# Anatomy of a modern Pharma spam campaign

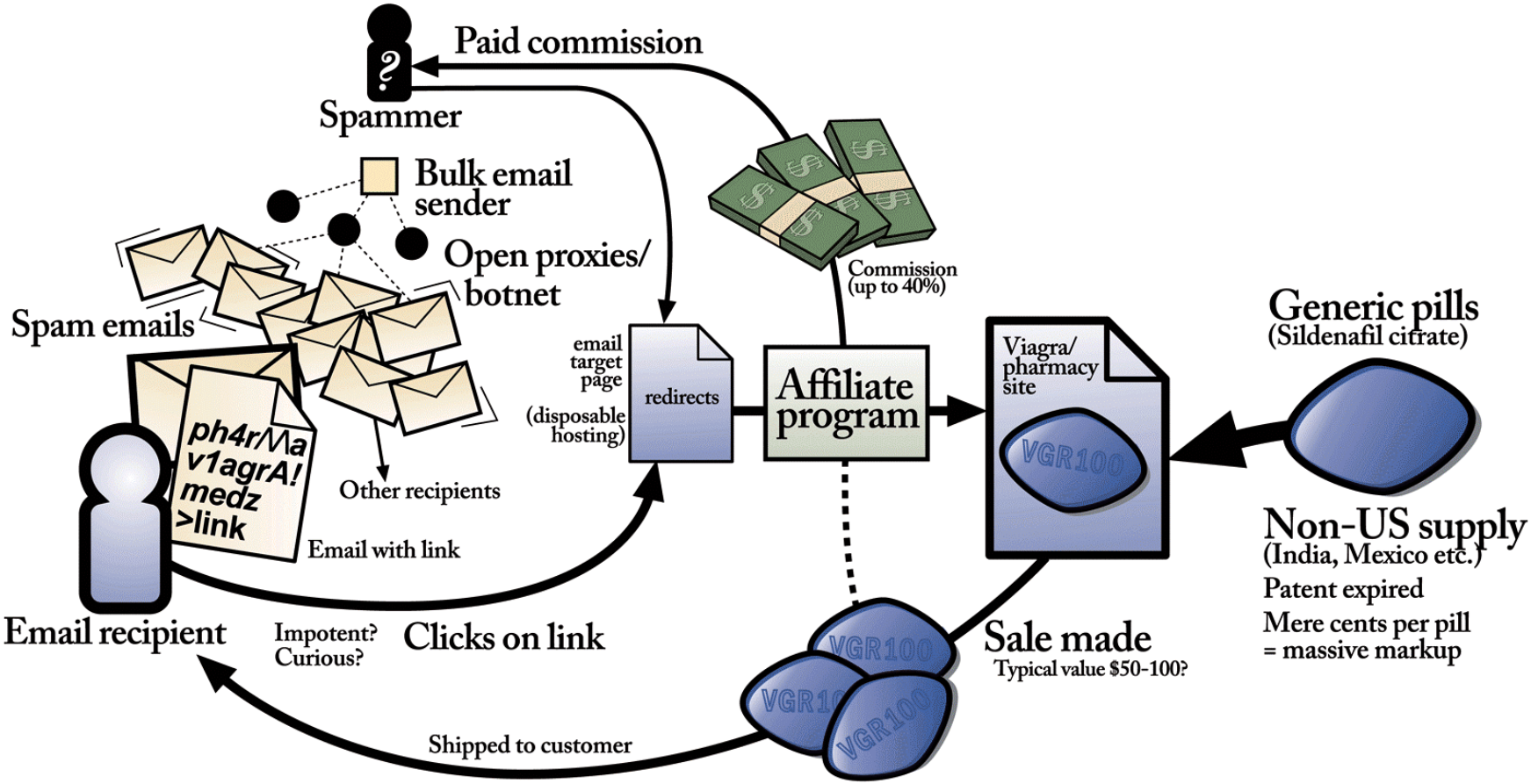



**Diagram by Stuart Brown**
**modernlifeisrubbish.co.uk**

# Life As A Spammer …

- From a research study where we infiltrated Storm and measured its use for spamming:
  - 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**