

Cybercrime / The Underground Economy

CS 161: Computer Security

Prof. David Wagner

April 30, 2013

Announcements

- **Final exam** in Hearst Gym, 5/14, arrive by 7PM
 - Last names A-L: 230 Hearst Gym
 - Last names M-Z: 237 Hearst Gym
- Course surveys at end of Friday's lecture: please attend!
- Review sessions next MWF 3-4pm here, with TAs
 - Monday 5/5: Network security
 - Wednesday 5/7: Web security
 - Friday 5/5: Cryptography

Goals For Today

- A look at **profit-driven cybercrime ...**
 - Monetization of malware
 - Monetization of spam
- ... including the *Underground Economy*
 - Elements
 - Significance
 - Infiltration/disruption

Cybercrime



Discussion

- Suppose you've hacked a bunch of machines. How could you make money from this?

Monetizing Malware on 1 Machine

- General malware monetization approaches:
 - Keylogging: steal financial/email/social network accounts
 - Ransomware
 - Scareware (“fake AV”)

System scan progress



Shared Documents

97 trojans



My Documents

334 trojans

Hard drives



Local Disk (C:)

353 trojans



Local Disk (D:)

78 trojans

DVD



DVD-RAM Drive (E:)



Scan procedures finished. 431 Probably harmful items were found.



Your Computer is Infected!

Threats and actions:

Name	Risk level	Date	Files infected	State
Email-Worm.Win32.Net	Critical	11.18.2008	36	Waiting removal
Email-Worm.Win32.Myd	Critical	11.18.2008	65	Waiting removal
Win 32:Delf-XQ	Critical	11.18.2008	44	Waiting removal

Description:

This program is potentially dangerous for your system. **Trojan-Downloader** stealing passwords, credit cards and other personal information from your computer.

Advice:

You need to remove this threat as soon as possible!



<http://protection-check07.com>

Potentially dangerous software. These programs may damage your computer and steal your private information. Online Security Checker needs Personal Antivirus components to repair your computer. Please click Ok to download and install Personal Antivirus tool.

OK



<http://protection-check07.com>

Your computer remains infected by threats! They might lead to data loss and file structure damage, and needed to be healed as soon as possible.

Return to Personal Antivirus and download it securely to your PC.

Cancel

OK



Full system cleanup

Monetizing Malware on 1 Machine

- General malware monetization approaches:
 - Keylogging: steal financial/email/social network accounts
 - Ransomware
 - Scareware (“fake AV”)
 - *Transaction generators* (“man-in-the-browser”)
 - 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 Large-Scale Malware

- Monetization that leverages *botnet scale*
 - DDoS (extortion)
 - Spam
 - *Click fraud*
 - Scam **infrastructure**
 - Hosting web pages (e.g., phishing)
 - Redirection to evade blacklisting/**takedown** (DNS)
 - Proxying traffic to thwart tracing / provide *IP diversity*
- Which of these cause serious pain for infected user?
 - **None**. Users have **little incentive** to prevent
 - ⇒ **Externality** (cost one party's actions impose on another)

Spam & Spam Profit

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 it: brand holders

Anatomy of a modern Pharmaceutical spam campaign

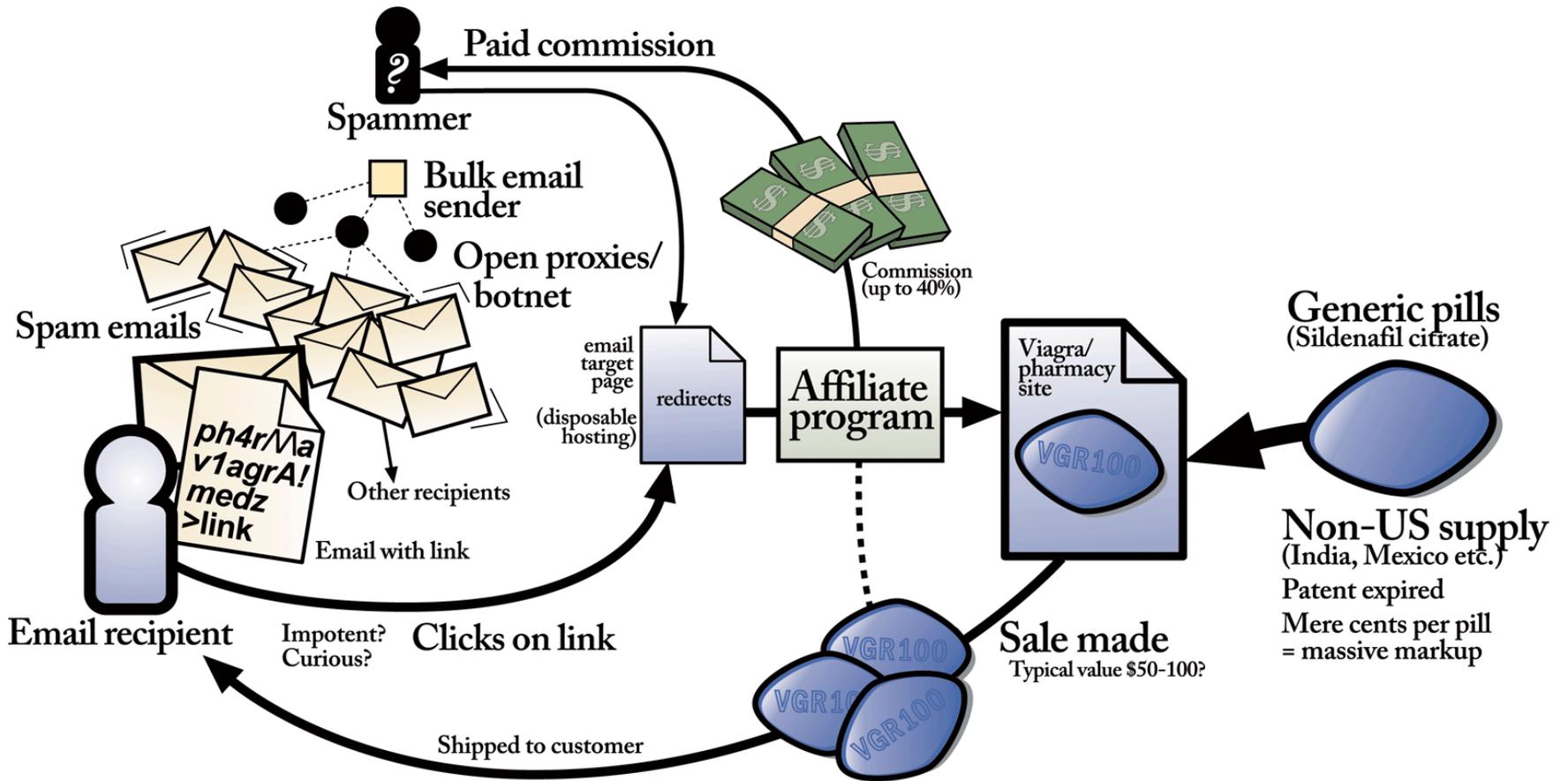


Diagram by Stuart Brown
modernlifeisrubbish.co.uk

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 it: 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, cont.

- 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, reshippers
 - Profit angle: enables profiting from cybercrime
 - Opponents: ?

Monetizing Spam, cont.

- Scheme #3: scams
 - Examples: pen pal relationships, 419 (“Nigerian”)
 - Profit angle: con victim into sending money
 - Oppo Money mules take incoming (fraudulent) financial transfers to their bank accounts, wire-transfer 90% out of country, keep 10% (19eater.com)
- Scheme #4: **recruiting** crooks/underlings
 - Examples: money mules, reshippers
 - Profit angle: enables profiting from cybercrime
 - Opponents: ?

Monetizing Spam, cont.

- Scheme #3: scams
 - Examples: pen pal relationships, 419 (“Nigerian”)
 - Profit angle: con victim into sending money
 - Opponents: scam artists
 - Reshippers 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, **reshippers**
 - Profit angle: enables profiting from cybercrime
 - Opponents: ?

Monetizing Spam, cont.

- 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: ?

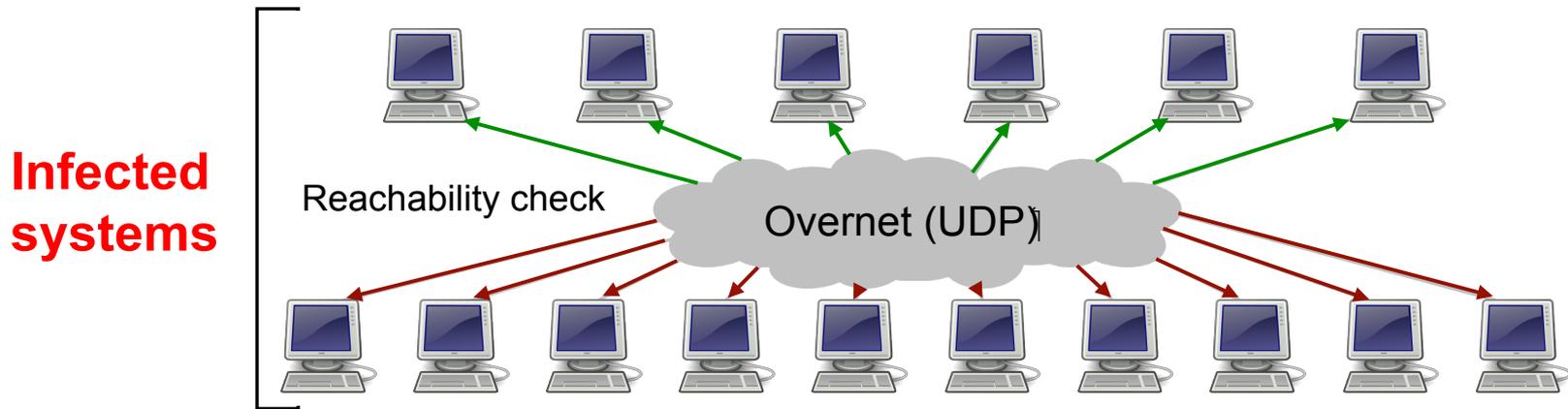
Welcome to Storm!



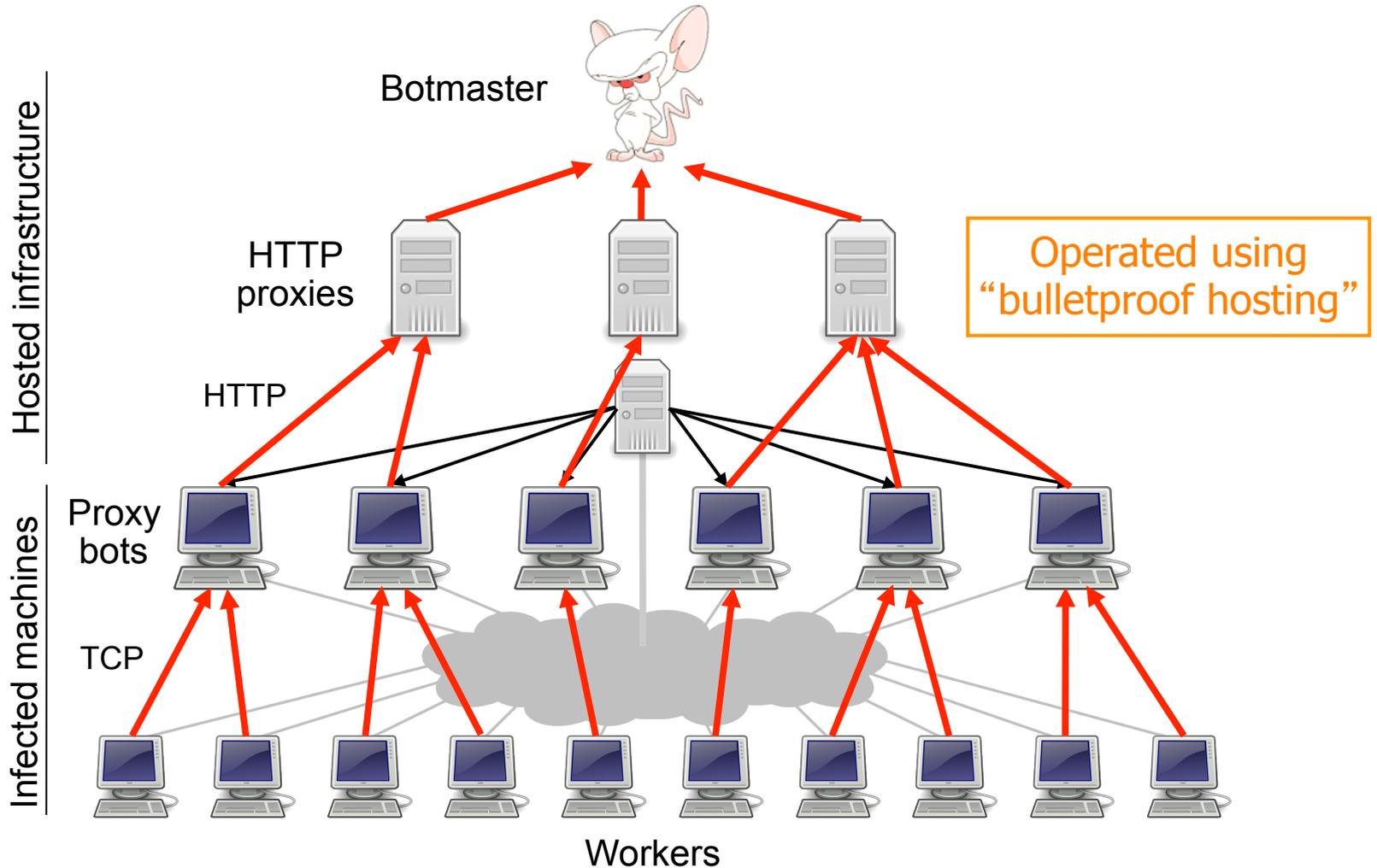
Would you like to be one of our newest bots?
Just read your postcard!

(Or even easier: just wait 5 seconds!)

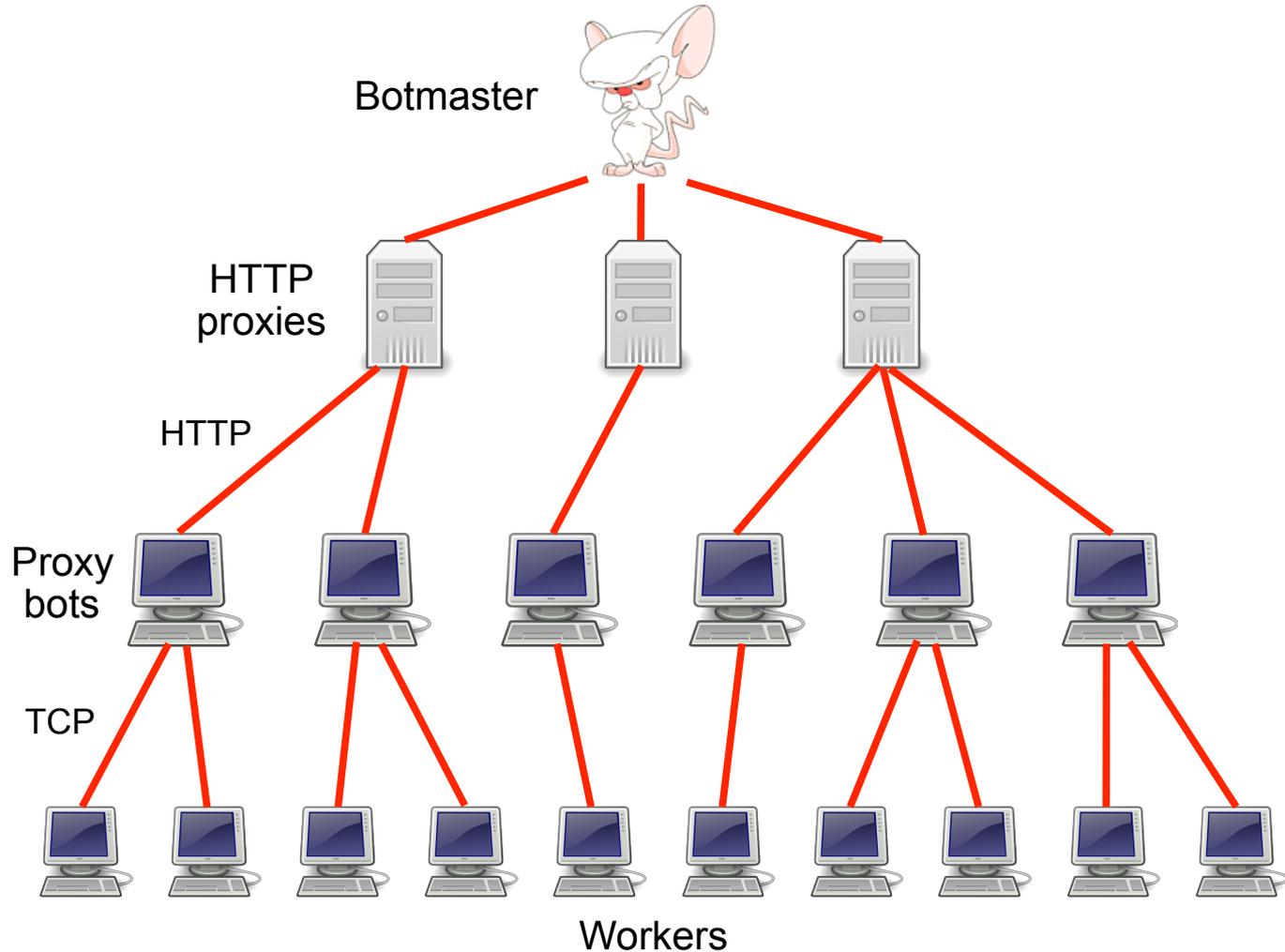
The *Storm* Spambot



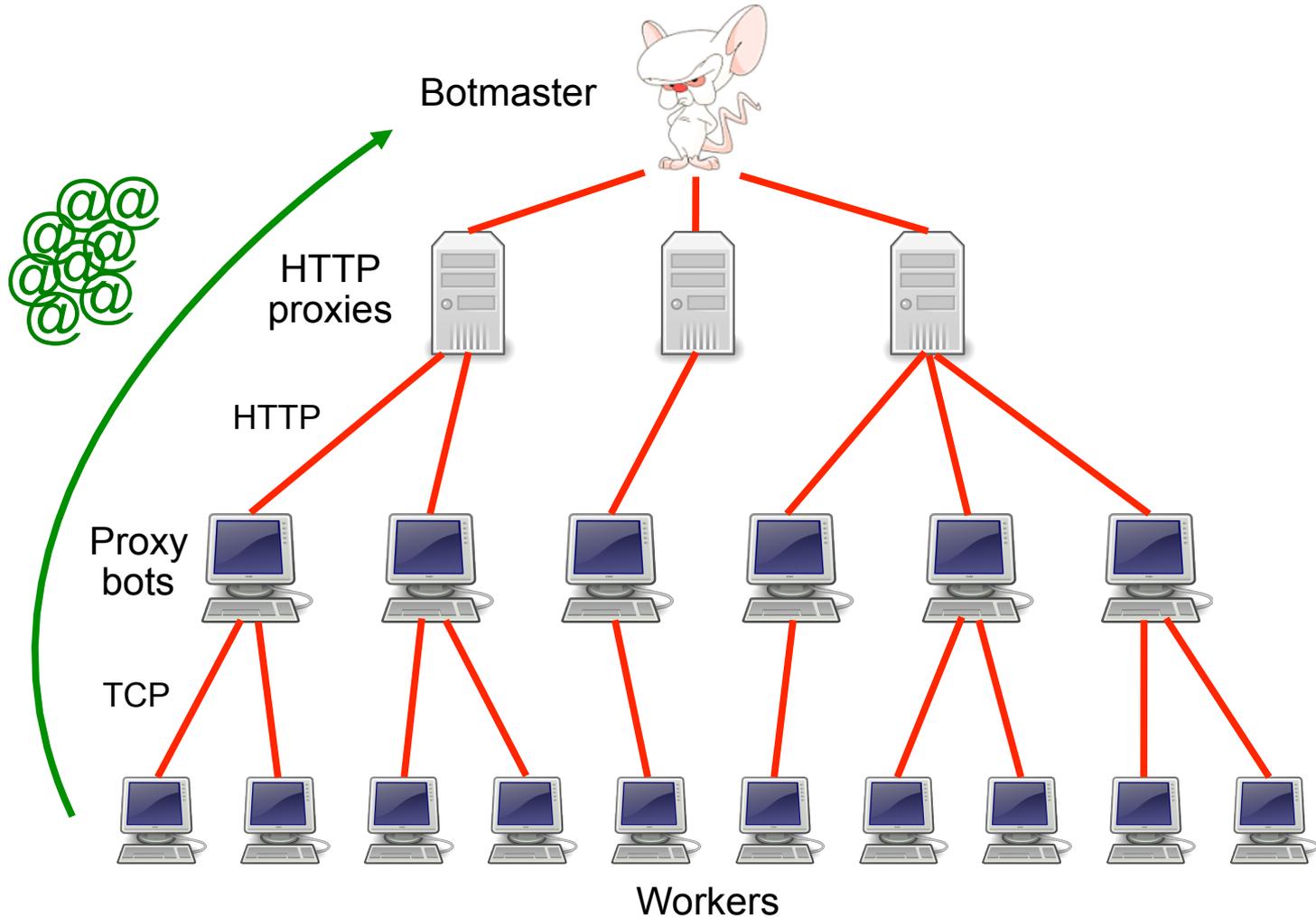
The Storm Botnet



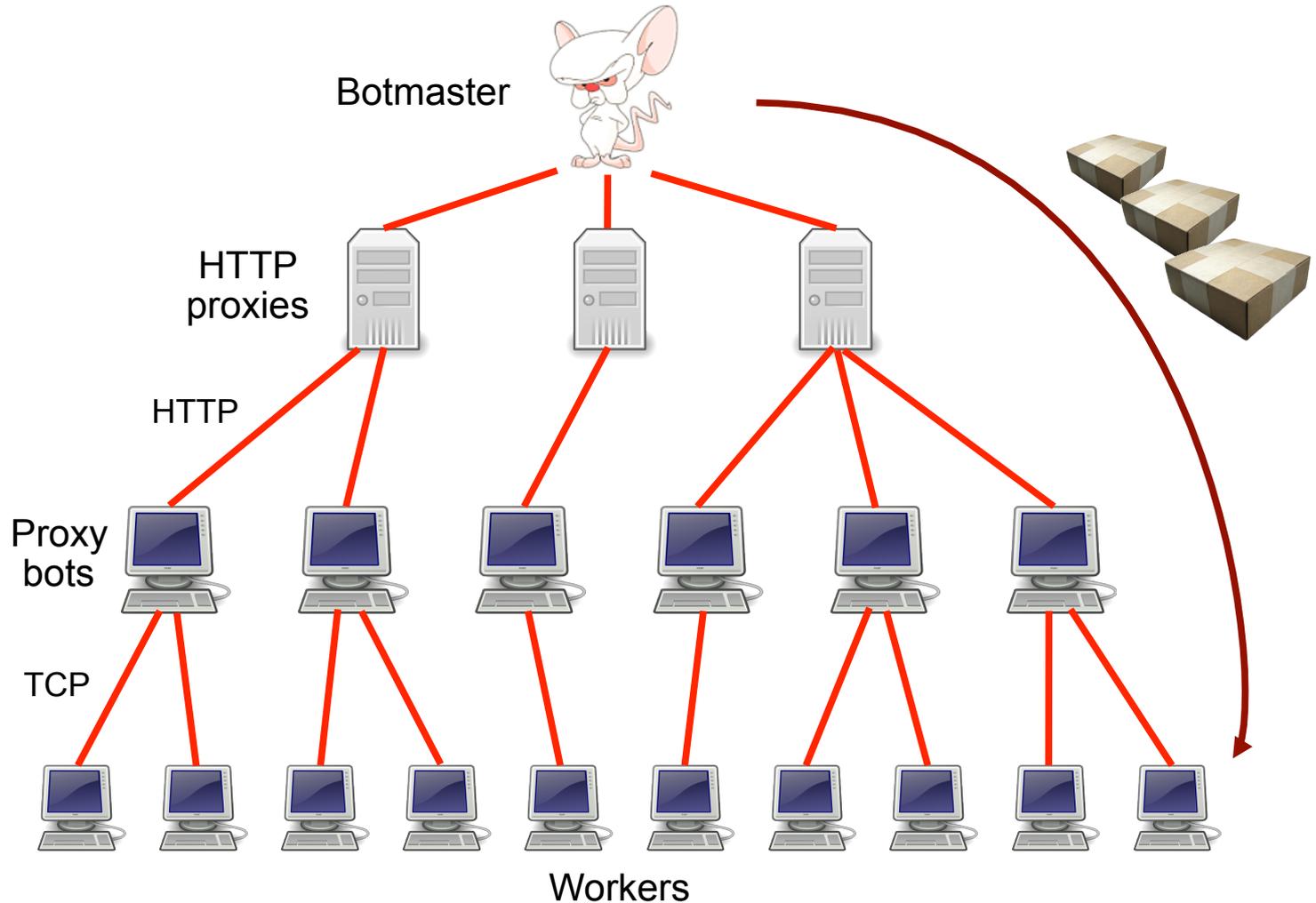
Spam “Campaign” Mechanics



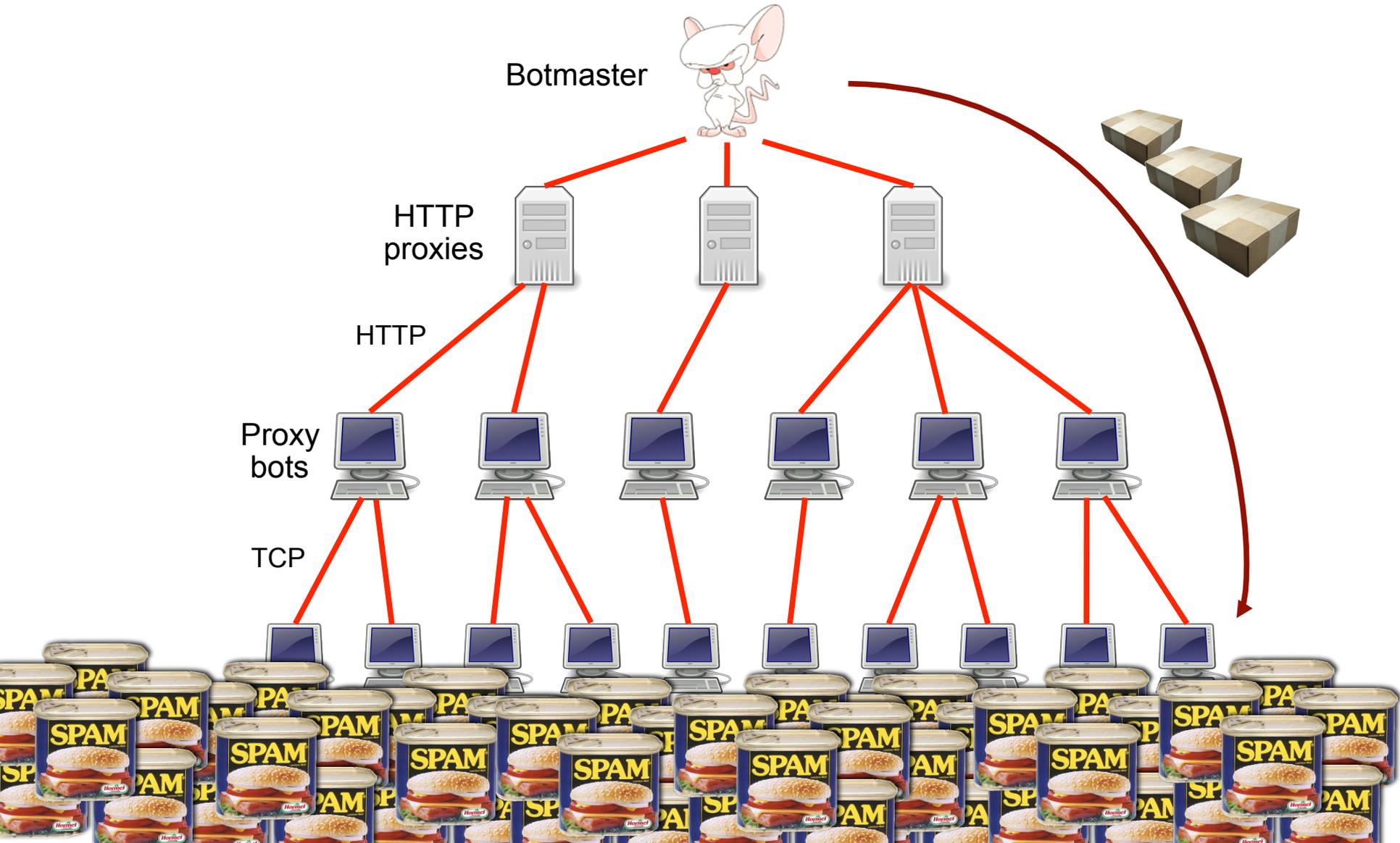
Campaign Mechanics: Harvest



Campaign Mechanics: Spamming



Campaign Mechanics: Spamming



**The Rise of the
*Underground Economy***



My Documents

ProAgent V2.0 Public Edition

Send Menu

- Send Passwords
- Send CD-Keys
- Send KeyLog
- Send System Information
- Send Address Book
- Send URL History
- Send Processes Log

Options

- Give a fake error message
- Melt server on install
- Disable AntiVirus Programs
- Clear Windows XP Restore Points
- Protection for removing Local Server

Server Icon

You can choose any icon for server



Choose Icon

Bind with File

Bind with File

You can bind server with any files you want



Select File To Bind

Notification

Your e-mail address which you will to receive information from ProAgent.

E-Mail:

ProAgent - Professional Agent Copyright © 2005 SIS-Team



Recycle Bin



ProAgent



9:56 AM

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

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



~~\$180.95~~ **\$140.00**

MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager
(Winsock)



~~\$360.95~~ **\$320.00**

YouTube Accounts Creator



~~\$120.95~~ **\$95.00**

Friendster Accounts Creator



~~\$120.95~~ **\$95.00**

Hi5 Accounts Creator



~~\$120.95~~ **\$95.00**

TopWorld Accounts Creator



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

BuyAccs.com

СЕРВИС РЕГИСТРАЦИИ АККАУНТОВ

Наш магазин аккаунтов рад предложить аккаунты различных **почтовых служб** и **бесплатных хостингов** для любых задач. Вы получите аккаунты **СРАЗУ после оплаты** заказа через Webmoney.

Также доступна услуга залива редиректов на **Pochta.ru**, **Cwahi.net** и **Ocatch.com** что является уникальной услугой - вы получаете готовые редиректы в течение часа после заказа. При покупке аккаунтов менее 1000 штук действует специальный тариф.

www.FreedomScripts.org - разработка софта на заказ

[Мега Софт для дорвеев - Zerber](#)

[Одобрятел друзей - Мой мир](#)

[Twidium](#) - безопасный и профессиональный инструмент для раскрутки твиттера
накрутить фолловеров в Твиттер

[Заработай на продаже аккаунтов](#)

[Купить аккаунты Одноклассников](#)

[Купить аккаунты Вконтакте](#)

Сейчас в продаже

Служба	Кол-во акков	Цена за 1K аккаунтов
Mail.ru	117025	до 10К: \$5 от 10К до 20К: \$4.5 от 20К: \$4
Mail.ru Mix	327199	до 10К: \$5 от 10К до 20К: \$4.5 от 20К: \$4
Mail.ru Second Hand	0	до 10К: \$4 от 10К до 20К: \$3.5 от 20К: \$3
Mail.ru Mix S/H	15811	до 10К: \$4 от 10К до 20К: \$3.5 от 20К: \$3
Yandex.ru	4758	до 10К: \$20 от 10К до 20К: \$19 от 20К: \$18
Narod.ru	5315	до 10К: \$50 от 10К до 20К: \$50 от 20К: \$50

Новости

06 Apr 2013

Временно не продаем аккаунты
Twitter.com

15 Mar 2013

Отличная цена на аккаунты
Facebook.com! Всего **\$80** за **1000 шт.**
Дешевле не бывает!

07 Фев 2013

Сенсационная цена на аккаунты
Yahoo.com. Теперь отличные аккаунты **со всеми регистрационными данными** по цене **от \$7** за **1000 шт!**

06 Фев 2013



Список доступных акков

Сервис по продаже аккаунтов аукциона eBay.

Добрые юзеры аукциона 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 субъективно.

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\$

Advertisement

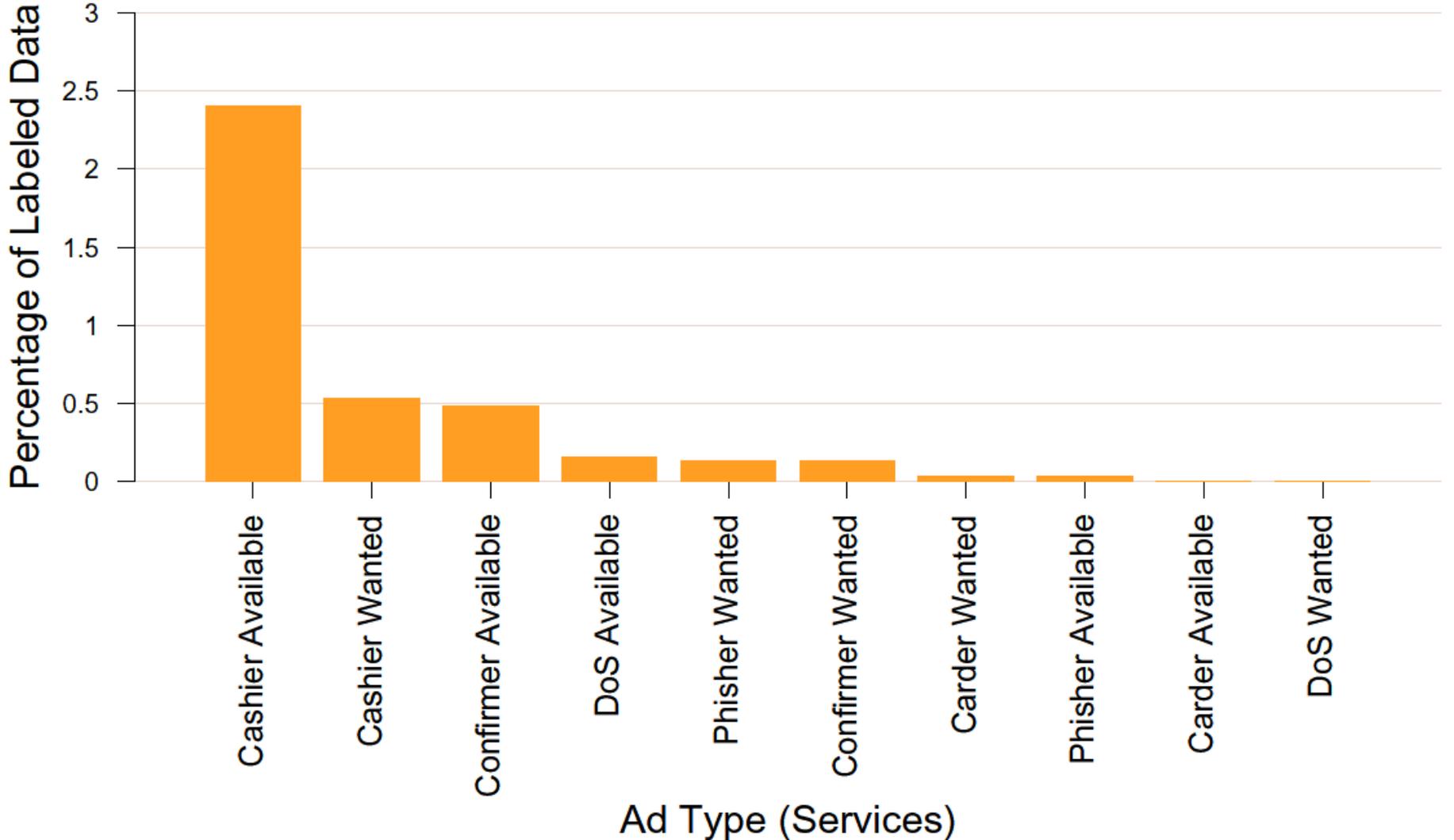
i have boa wells and barclays bank logins....

have hacked hosts, mail lists, php mailer send to all inbox

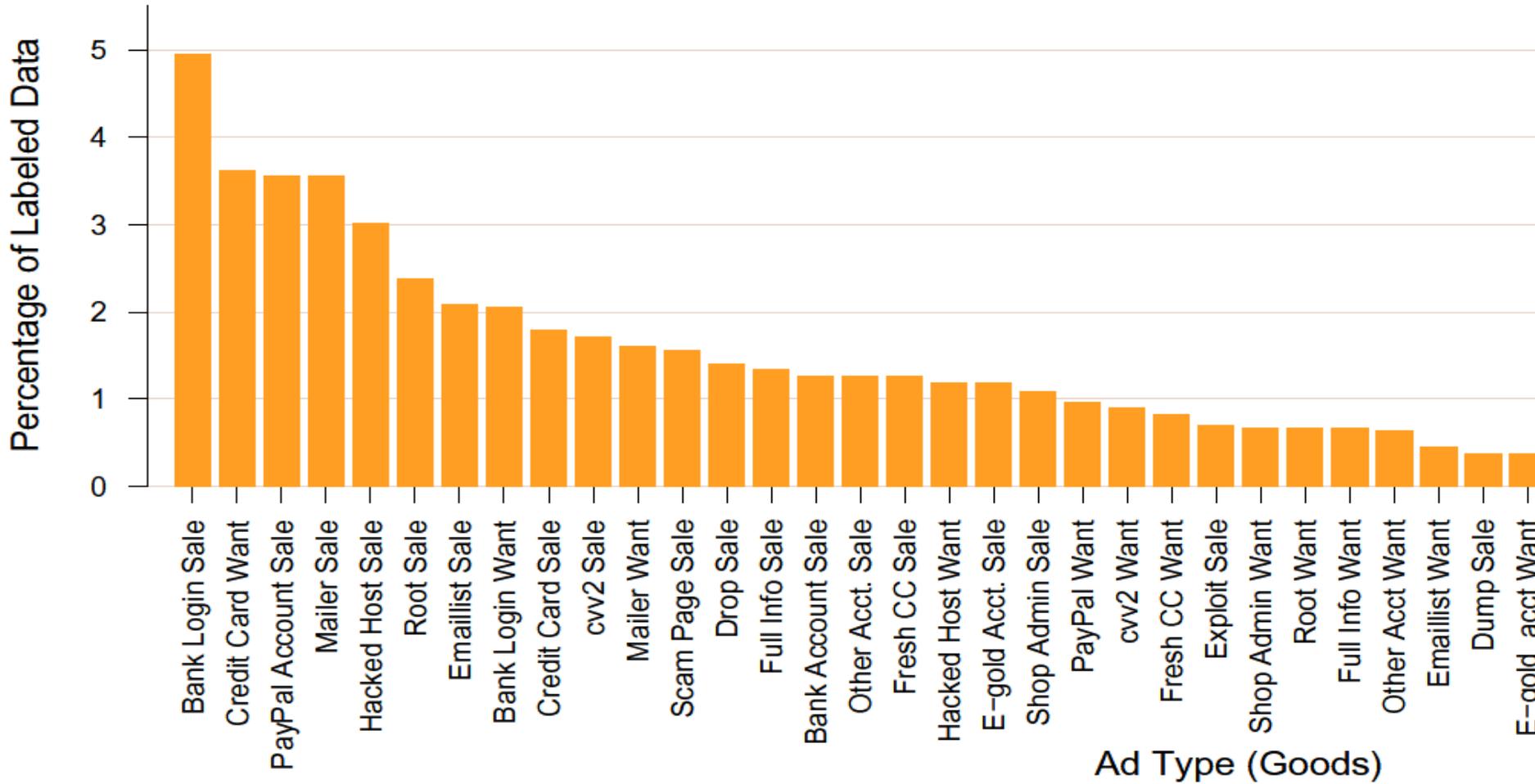
i need 1 mastercard i give 1 linux hacked root

i have verified paypal accounts with good balance...and i can cashout paypals

Marketplace Ads for Services



Marketplace Ads for Goods



Pay-Per-Install (PPI)

Installs4Sale.net - надежный сервис по загрузкам, достойный доверия



КОНТАКТЫ

560869831

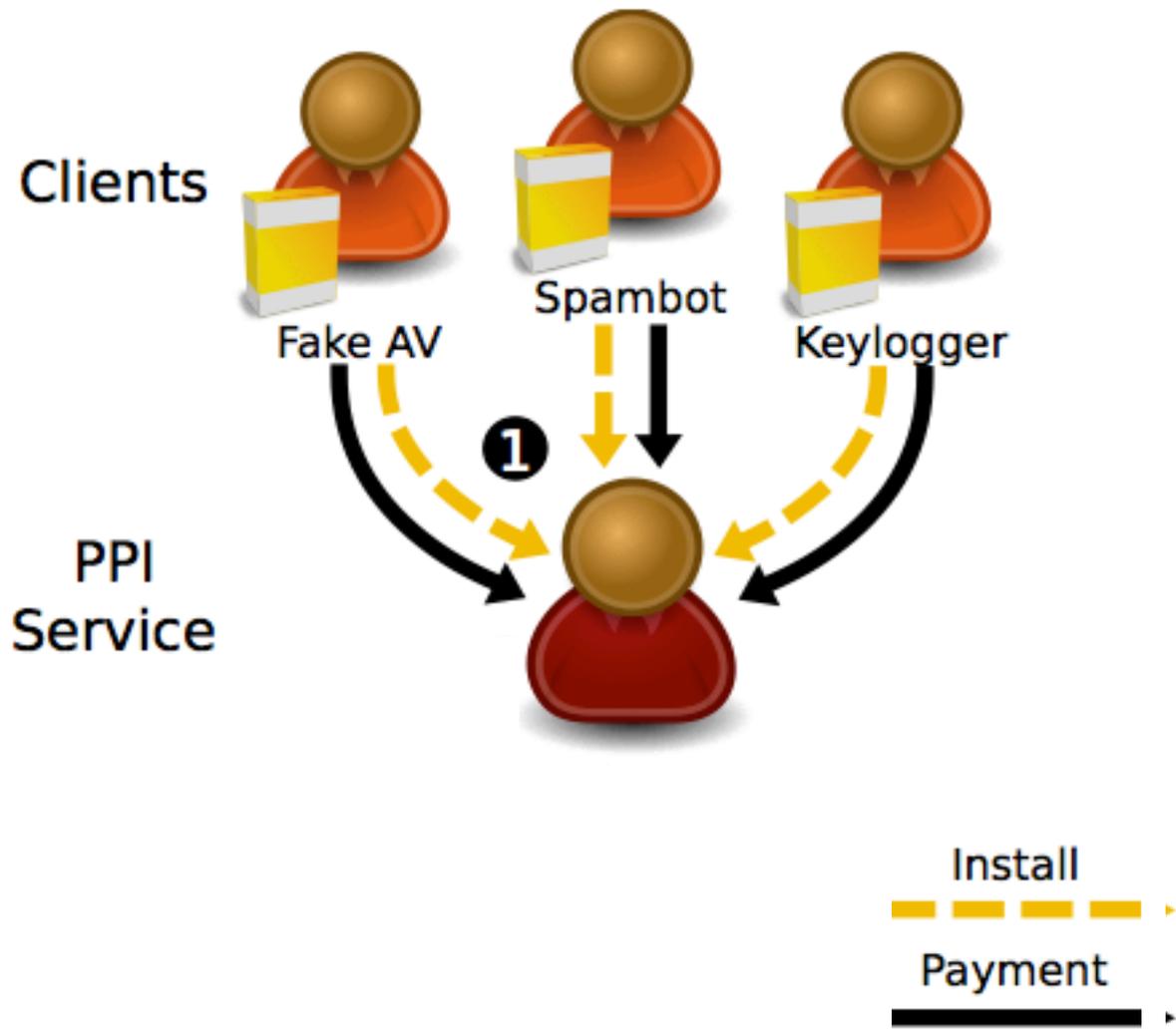
550525933

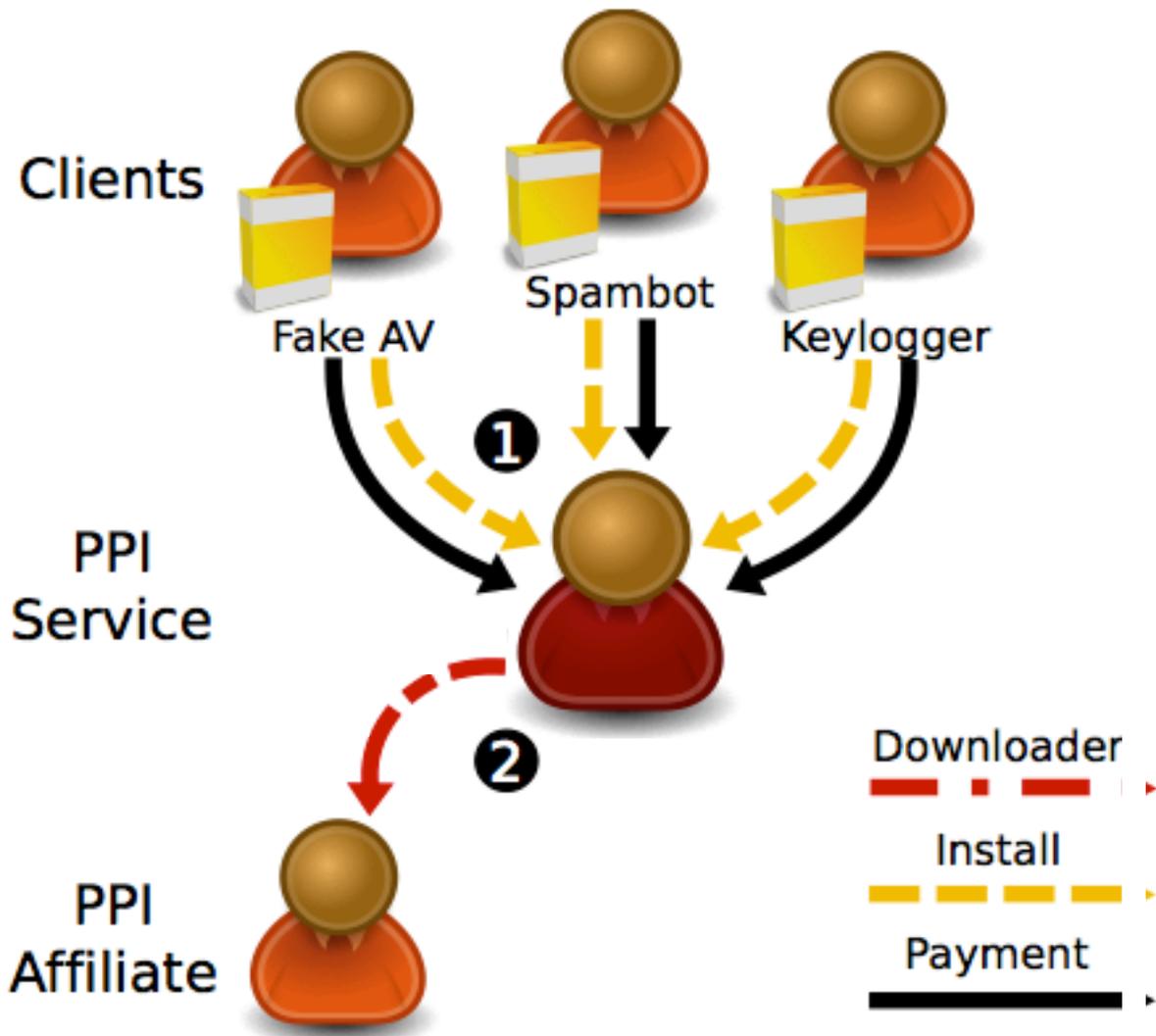
info [at] installs4sale.net

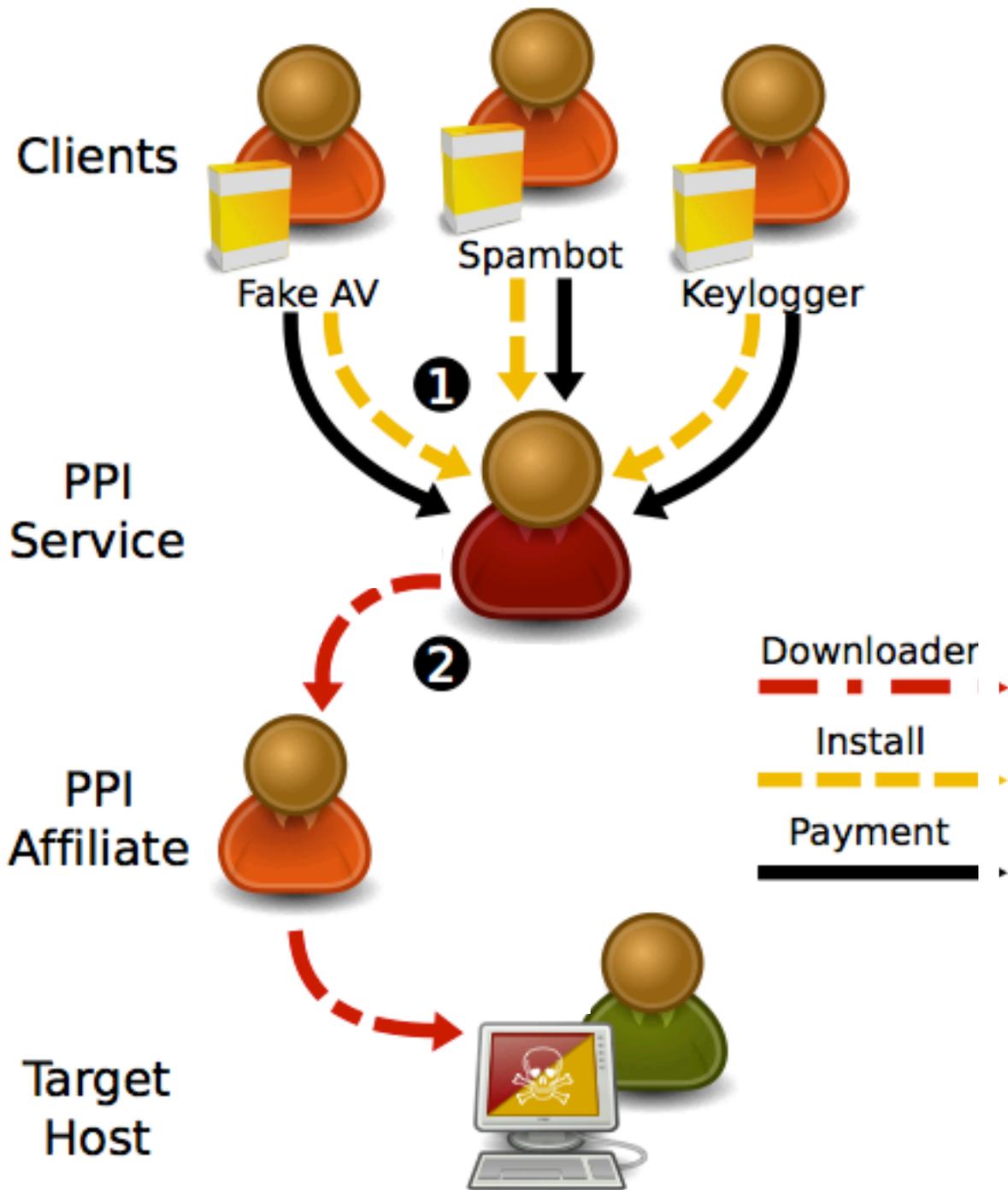
ПРИЕМУЩЕСТВА

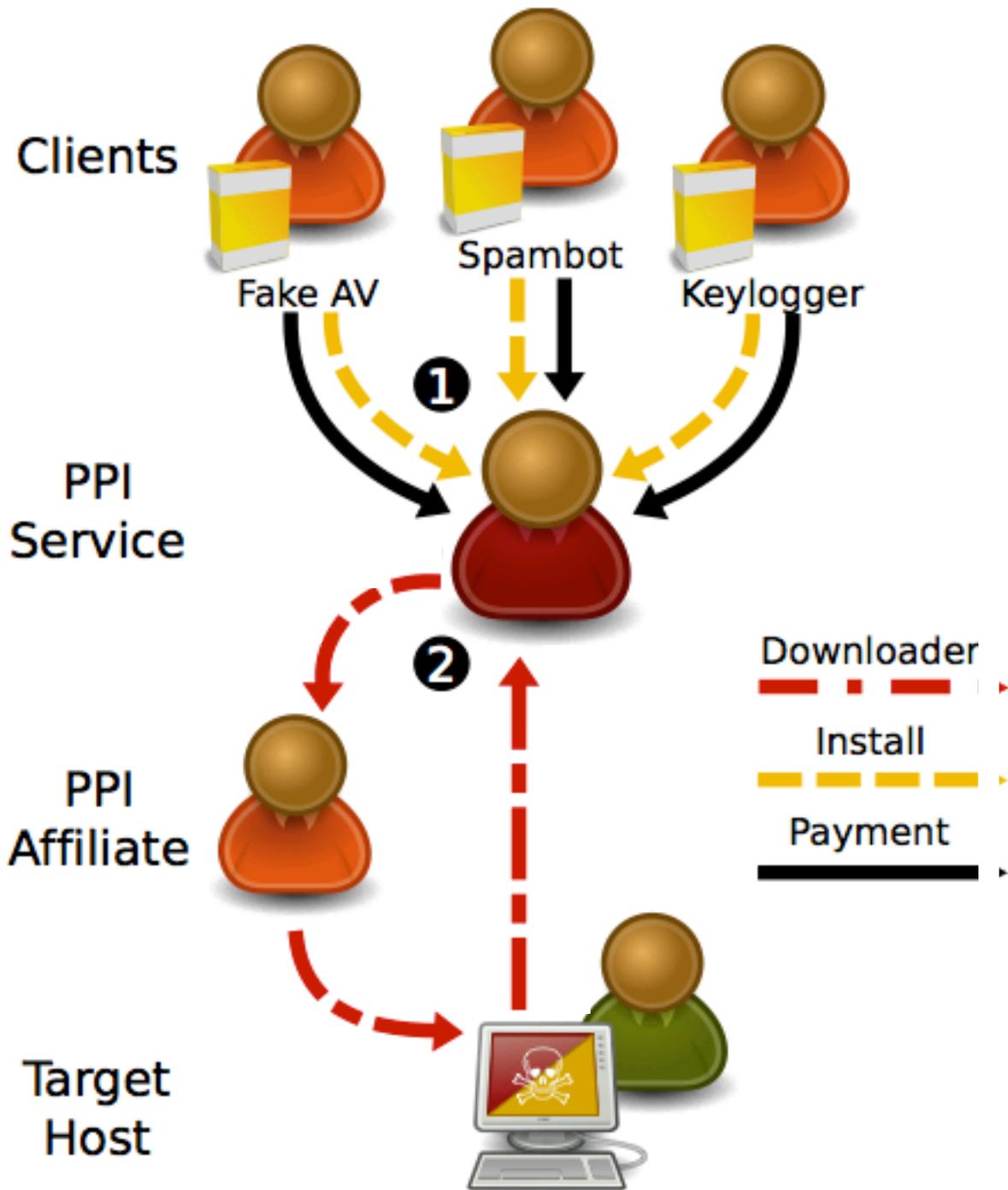
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!

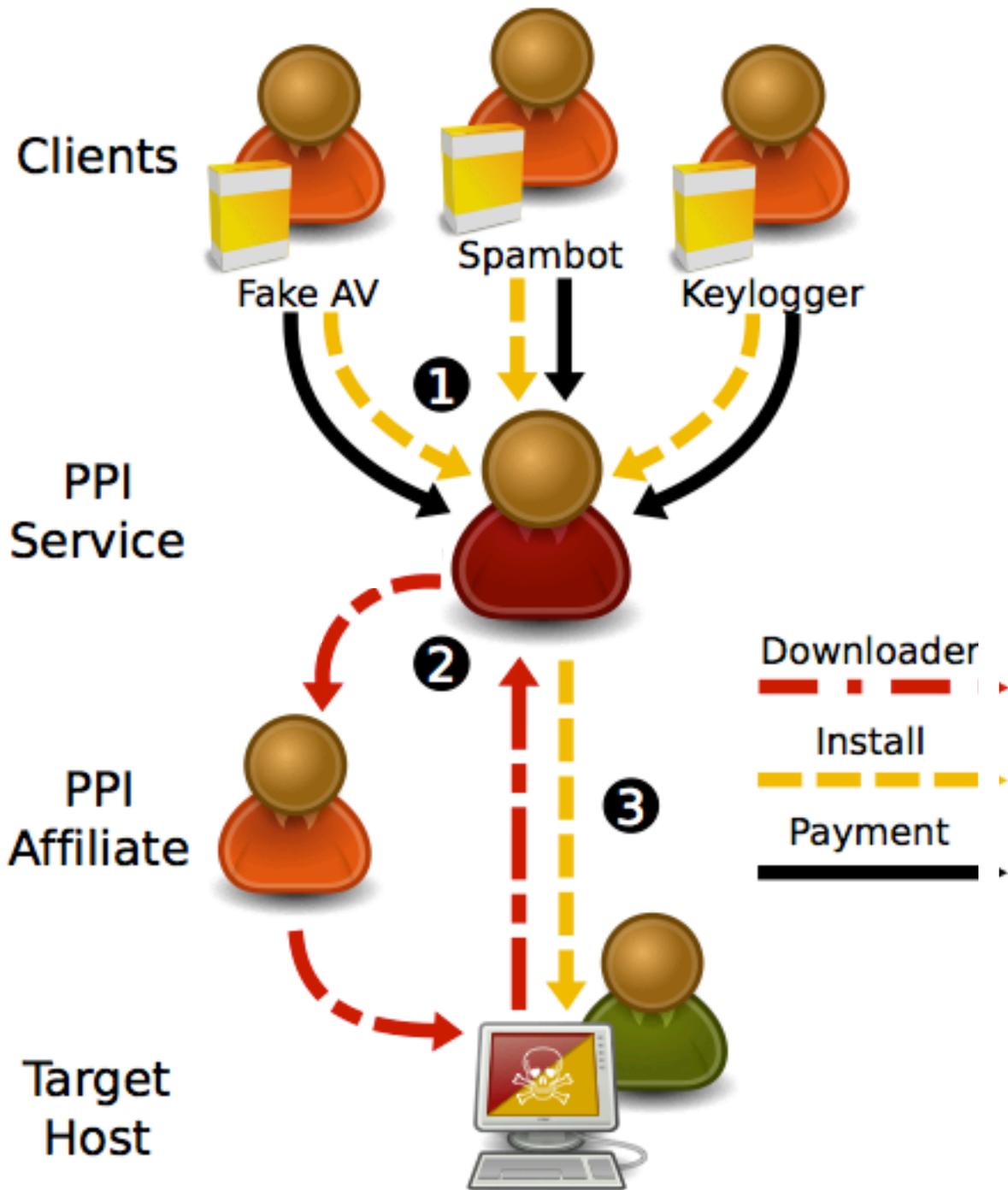


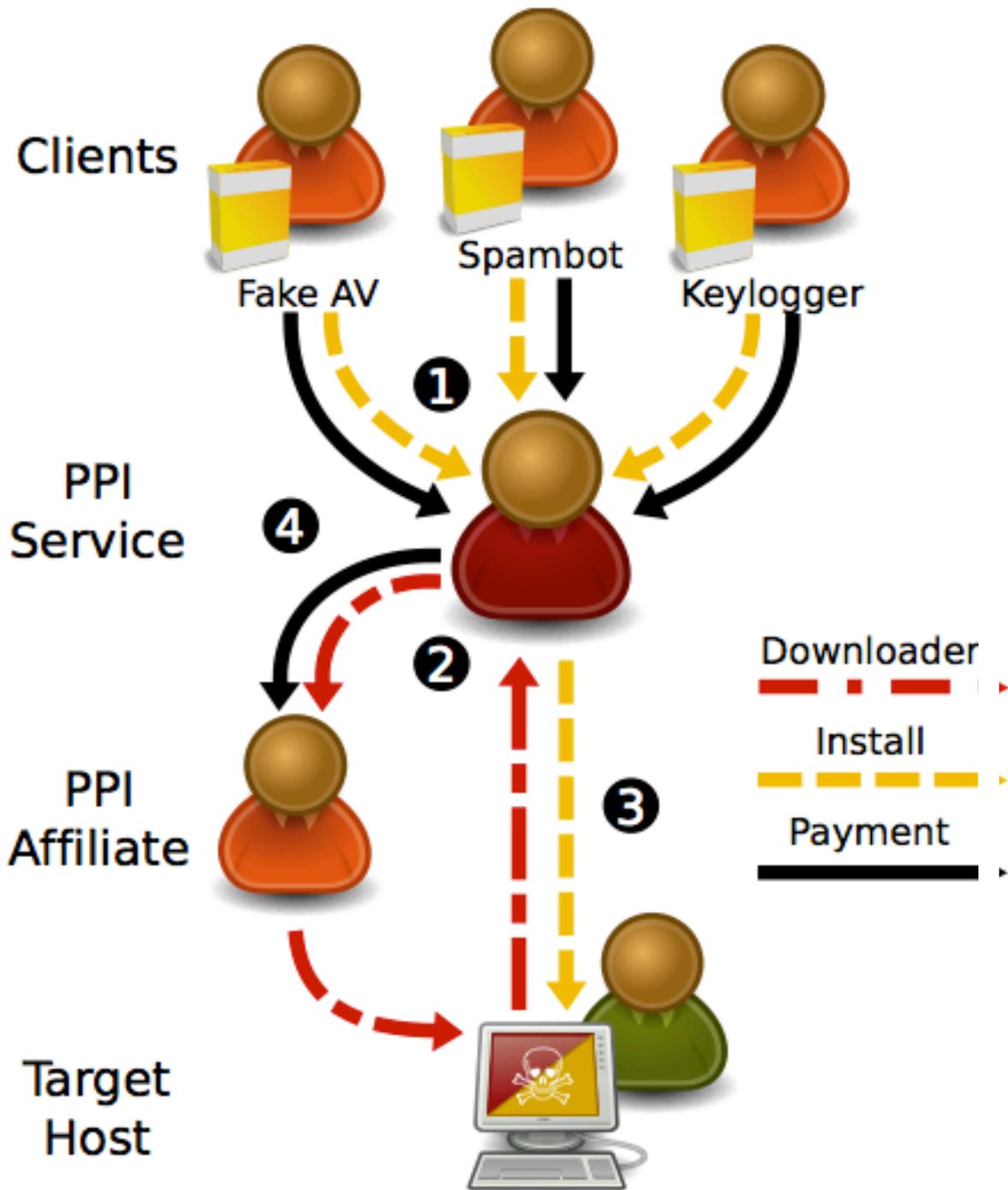














Home

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!

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\$

Defenses

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, cont.

- 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*

Life As A Spammer ...

- 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

Life As A Spammer ...

- Storm infiltration study found:
 - Modern spam campaigns can send 10s of billions of

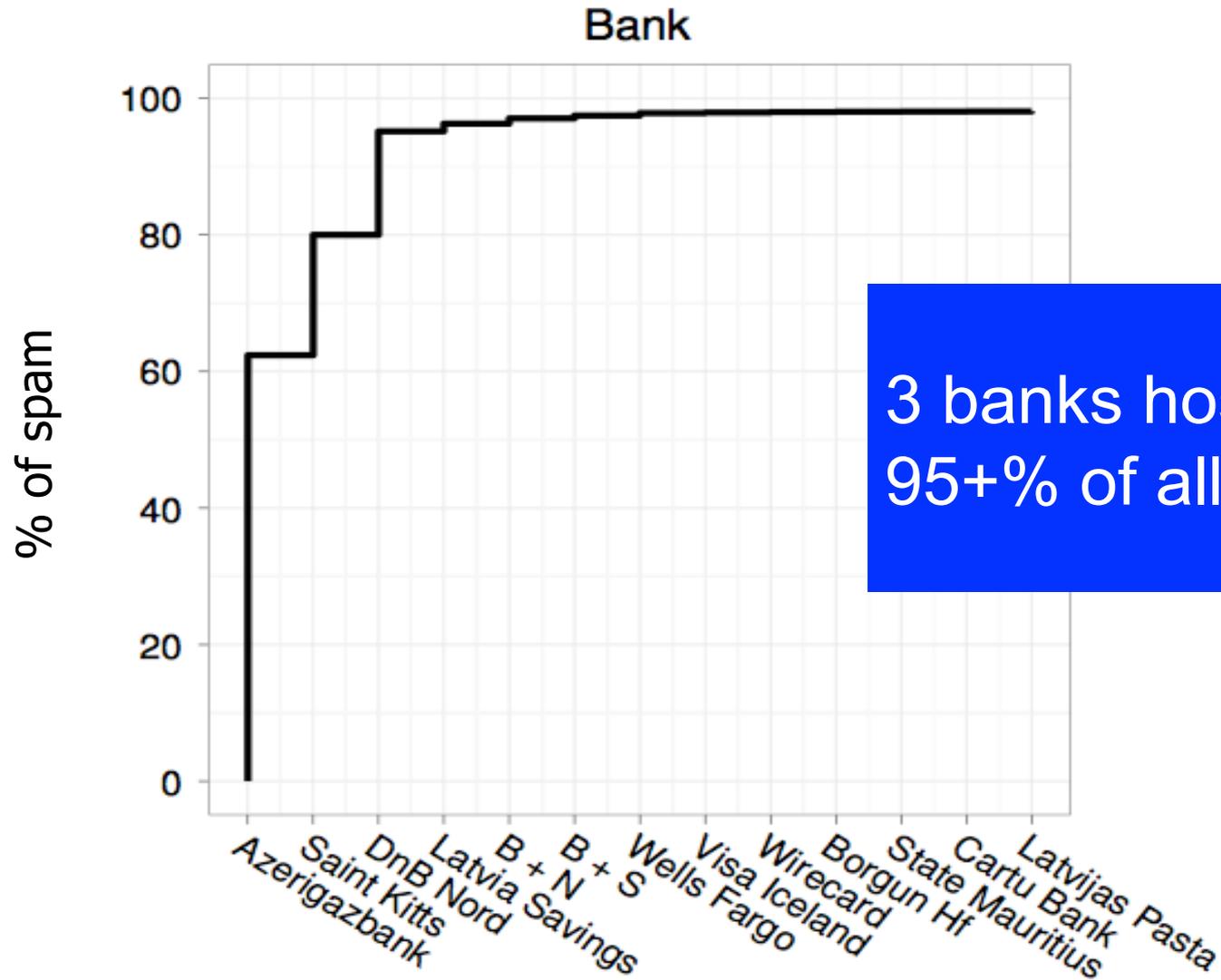
Another study based on making purchases of spam-advertised pharmaceuticals found that 3 merchant banks hosted **95+% of all sales** ...

... suggesting a novel way to suppress spam is to *undermine the credit-card processing*

- 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

Merchant Bank bottlenecks





Уважаемые Вебмастера,

В связи с событиями произошедшими в течение последних двух месяцев, когда под удар попали все банковские и процессинговые счета компании, мы вынуждены сообщить, что, поскольку до сегодняшнего дня не удалось найти достаточно надежного решения для продолжения работы, а долги перед поставщиками и партнерами продолжают расти, мы вынуждены полностью остановить функционирование партнерской программы Medinc.

Мы были рады работать с вами, друзья, и нам жаль, что сотрудничество в рамках данного проекта более невозможно.

В случае, если нам удастся найти надежное, по нашему мнению, процессинговое решение и возобновить работу, все вебмастера получат уведомления на почтовые адреса, указанные при регистрации.

Dear webmasters,

Due to the recent developments which led to all our bank and processing accounts being jeopardized, we have to inform you, that functioning of the Medinc partnership program will be discontinued, as no reliable solution has been found to keep it working, and the debts to suppliers and partners keep increasing.

We were happy to work with all of you, and we are very sorry that we can't cooperate with you anymore within this project.

If we manage to find a reliable processing solution to resume working, all webmasters will receive an email notification sent to the address submitted during registration.



Post Reply

Страница 1 из 2 1 2 >

29-06-2012, 23:28

Опции темы Опции просмотра

funny_duck

ВАЖНО: переход в режим "ПАУЗА"!

Регистрация: 23-05-2007
Сообщений: 273

Уважаемые Партнеры,

Как вы могли заметить, последние пару дней у нас проблемы с процессингом. Решение вопроса "подвисло" в воздухе, и пока не ясны окончательные сроки его разрешения.

Мы принципиально не хотим собирать "вейтинги" и по сути работать в батч. Мы так же не готовы рисковать вашими деньгами с малоознакомыми и не очень серьезными посредниками. Поэтому с настоящего момента **весь ГлавМед переходит в режим "ПАУЗА"**. Никакие новые заказы обрабатываться не будут до момента решения вопроса с процессингом. Все уже запрошенные заказы будут выполнены, как и следует.

Убедительная просьба временно перевести свой трафик на другие шопы/проекты.

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.

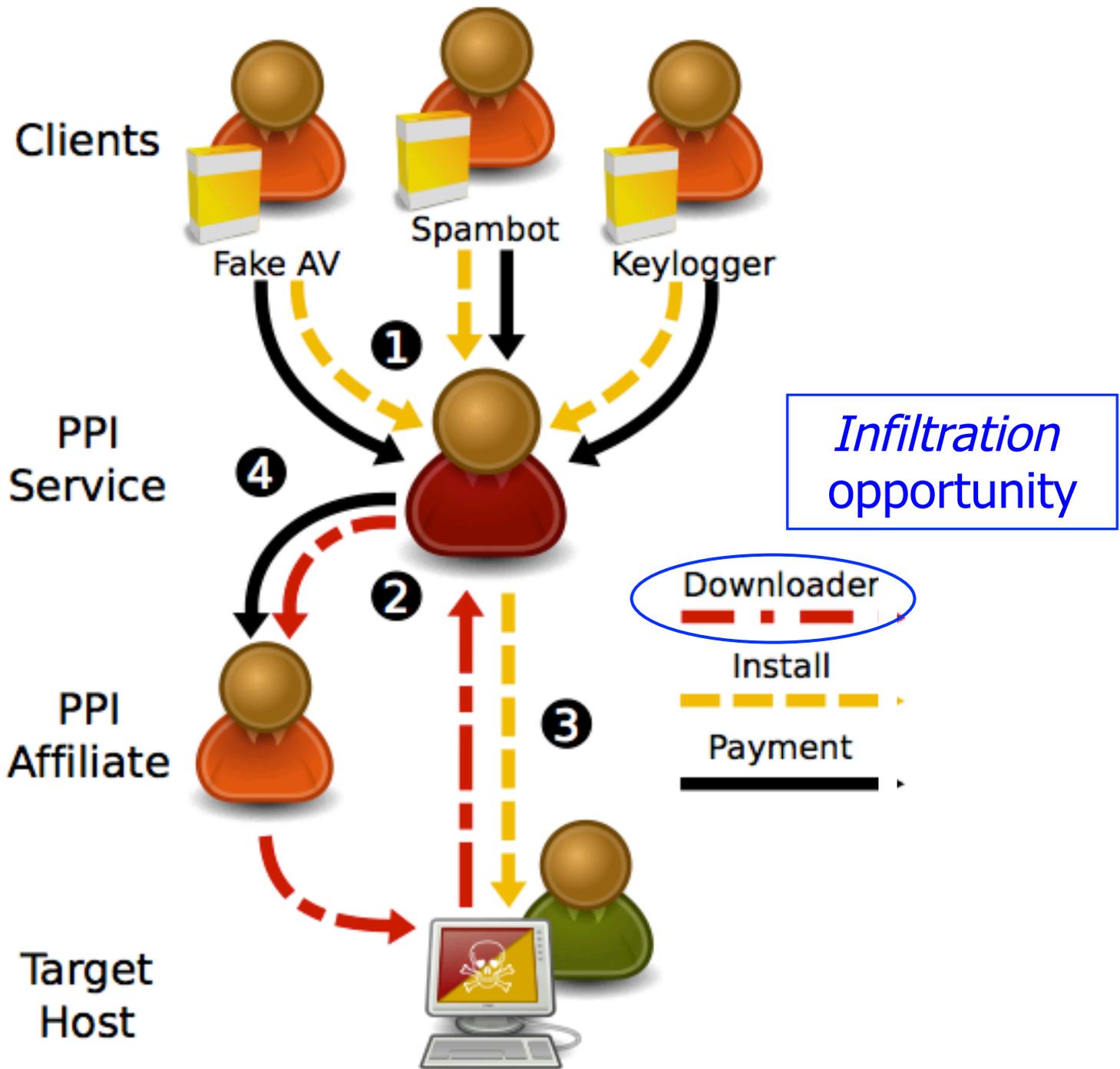
.....
We urge you to temporarily switch your traffic to other shops/projects.

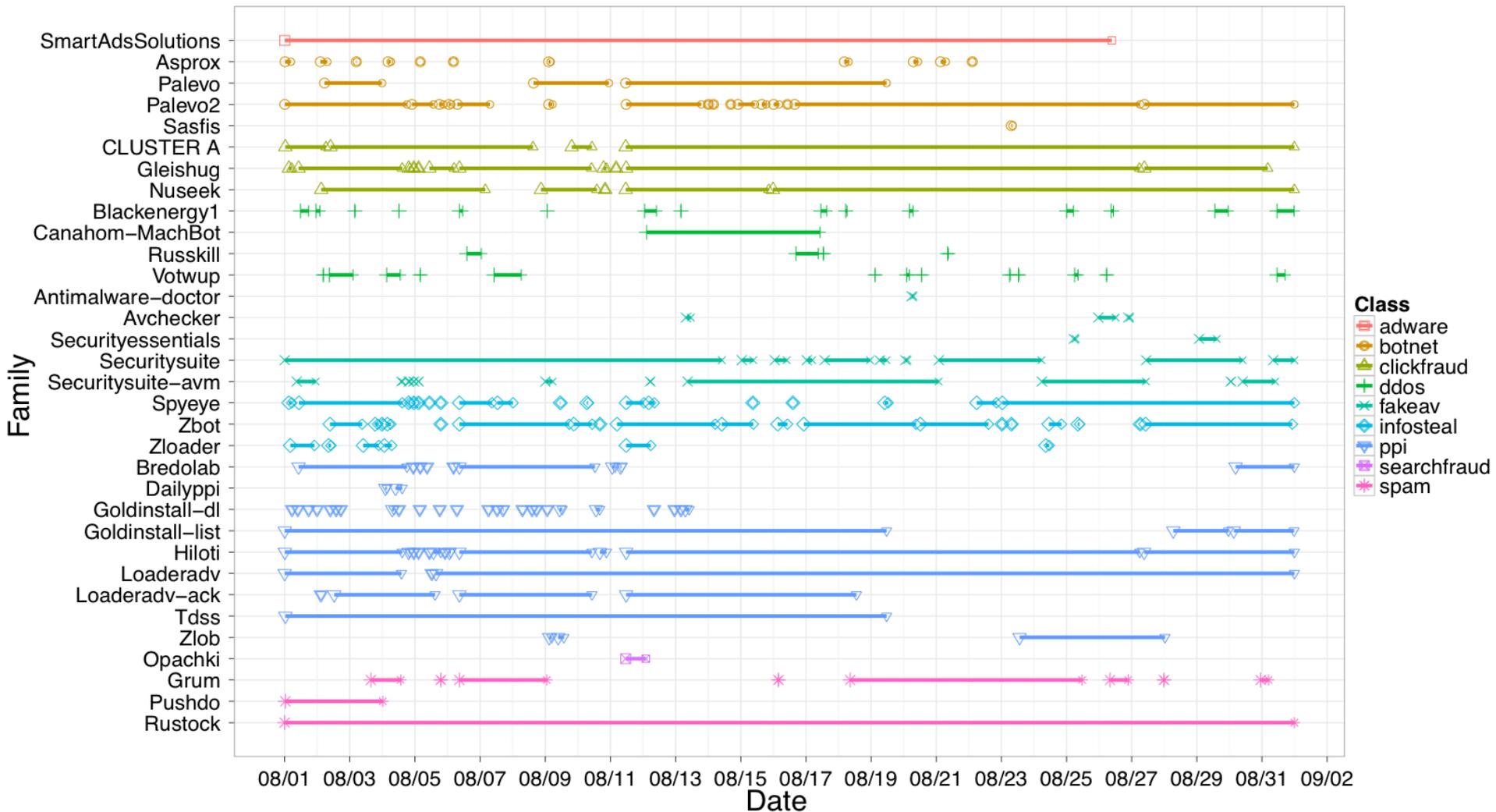
больше ясности и

елика, но в любом

щаться ко мне

Quote





Via protocol emulation, extracted (“milked”)
 > 1M malicious binaries over 6 months

	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		

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

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

BuyAccs.com

СЕРВИС РЕГИСТРАЦИИ АККАУНТОВ

Наш магазин аккаунтов рад предложить аккаунты различных **почтовых служб** и **бесплатных хостингов** для любых задач. Вы получите аккаунты **СРАЗУ после оплаты** заказа через Webmoney.

Также доступна услуга залива редиректов на **Pochta.ru**, **Cwahi.net** и **Ocatch.com** что является уникальной услугой - вы получаете готовые редиректы в течение часа после заказа. При покупке аккаунтов менее 1000 штук действует специальный тариф.

www.FreedomScripts.org - разработка софта на заказ

[Мега Софт для дорвеев - Zerber](#)

[Одобрятел друзей - Мой мир](#)

[Twidium](#) - безопасный и профессиональный инструмент для раскрутки твиттера
накрутить фолловеров в Твиттер

[Заработай на продаже аккаунтов](#)

[Купить аккаунты Одноклассников](#)

[Купить аккаунты Вконтакте](#)

Сейчас в продаже

Служба	Кол-во акков	Цена за 1K аккаунтов
Mail.ru	117025	до 10К: \$5 от 10К до 20К: \$4.5 от 20К: \$4
Mail.ru Mix	327199	до 10К: \$5 от 10К до 20К: \$4.5 от 20К: \$4
Mail.ru Second Hand	0	до 10К: \$4 от 10К до 20К: \$3.5 от 20К: \$3
Mail.ru Mix S/H	15811	до 10К: \$4 от 10К до 20К: \$3.5 от 20К: \$3
Yandex.ru	4758	до 10К: \$20 от 10К до 20К: \$19 от 20К: \$18
Narod.ru	5315	до 10К: \$50 от 10К до 20К: \$50 от 20К: \$50

Новости

06 Apr 2013

Временно не продаем аккаунты
Twitter.com

15 Mar 2013

Отличная цена на аккаунты
Facebook.com! Всего **\$80** за **1000 шт.**
Дешевле не бывает!

07 Фев 2013

Сенсационная цена на аккаунты
Yahoo.com. Теперь отличные аккаунты **со всеми регистрационными данными** по цене **от \$7** за **1000 шт!**

06 Фев 2013

BuyAccs.com

BUY BULK ACCOUNTS AT BEST PRICES

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 Liberty Reserve and Paypal.

Please, review our [terms and conditions](#) before purchasing any accounts.

[Buy Yahoo Account](#)

[Buy Twitter Account](#)

[Buy Livejournal Account](#)

[Buy Hotmail Account](#)

 For sale

Provider	Quantity	Rate for 1000
Hotmail.com	449292	1K-10K: \$5 10K-20K: \$4.5 20K+: \$4
Hotmail.com Verified	423418	1K-10K: \$6 10K-20K: \$5.5 20K+: \$5
Outlook.com Plus	9661	1K-10K: \$4 10K-20K: \$3.5 20K+: \$3
Gmail.com USA PVA	4340	1K-10K: \$100 10K-20K: \$95 20K+: \$90
Yahoo.com	14058	1K-10K: \$8 10K-20K: \$7.5 20K+: \$7
Yahoo.com USA	8688	1K-10K: \$15 10K-20K: \$15 20K+: \$15
Nokiamail.com	0	1K-10K: \$10 10K-20K: \$10 20K+: \$9

06 Apr 2013

Twitter accounts are not available. We will start selling them shortly.

06 Apr 2013

Twitter accounts are not available. We will start selling them shortly.

07 Feb 2013

Added **Instagram** accounts at a great rate: **\$50 per 1000**.

04 Dec 2012

Just added **Fully Profiled Twitter Accounts** at a great rate - **\$30 per 1000**. Accounts come with **avatar, bio and random background**.

19 Nov 2012

Great prices for wholesale **Twitter.com** and **Hotmail.com** orders!

Infiltration

~~ShadowCrew~~

Infiltrated
(Secret Service)

CarderPlanet

CardersMarket

~~DarkMarket~~

Infiltrated (FBI)

State-sponsored Adversaries

Russian election protests – Saturday 10 December 2011

- Largest political event of its kind since the fall of the USSR
- An estimated 50,000 people gathered in Moscow and 10,000 in St Petersburg
- They allege widespread fraud in Sunday's polls
- More than 1,000 arrests
- Protestors pledge to take to the streets again on December 24
- They want Sunday's election results annulled

#триумфальная
(#triumphal)



26K Twitter accounts tweet 440K junk messages to drown out discourse / coordination.

Geolocation of Logins



Nospam Logins

Geolocation of Logins



Nonspam Logins



Spam Logins

26K accounts purchased from *spam-as-a-service* program.
Part of a “lot” of 975K. Used ~20K distinct IP addresses.

Takeaways

- Rise of cybercrime is a major challenge for security, because adversaries have become far more capable...
- But cybercriminals are lazy and look for easiest way to make a buck. So, focus defenses on the easiest ways to turn a technical security breach into money.
- “Follow the money.”

Extra Material

Welcome to Storm! What can we sell you?

The screenshot shows the Canadian Pharmacy website interface. At the top, there's a navigation bar with links for Home, Bestsellers, All products, FAQ, and Contact us. A currency selector shows \$, €, and £, with a 'Pharma Bonus' icon. A shopping cart icon indicates 'Your cart: \$0.00 (0 items)' with a 'Proceed to Checkout' button.

The main banner features the Canadian Pharmacy logo and the tagline '#1 Internet Online Drugstore' alongside a photo of two doctors. Below this is a 'Products list' section with three featured items:

- Viagra + Cialis:** 10 x Viagra 100 mg and 10 x Cialis 20 mg. Price: 69⁹⁹\$.
- Growth Pack:** Growth Pills (1 bottle x 60caps) and Growth Oil (1 tube x 2oz). Price: 179⁹⁵\$.
- Viagra:** 120 pills 100 mg and +4 Free pills. Price: 225⁶¹\$.

Each product has an 'ORDER NOW' button. To the left of the products is a sidebar with a 'Bestsellers' section listing categories like Male Enhancement, Men's Health, SALES - 20% OFF, Female Enhancement, Weight Loss, Gums New!, Body-Building, and Hypnotherapy. Below the products is a search bar with a dropdown menu for 'Search by name' (A-Z) and a search input field.

At the bottom, there's a 'Today's Bestsellers' section featuring three products:

- Viagra:** Our price \$1.21.
- Cialis:** Our price \$2.18.
- Viagra Professional:** Our price \$3.73.

Each product in the 'Today's Bestsellers' section includes a 'More info' link and an 'Add to cart' button.





Kirill Levchenko

klevchen@cs.ucsd.edu

I am a project scientist with the [Systems and Networking](#) group in the Computer Science department at the University of California, San Diego. My current research

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**

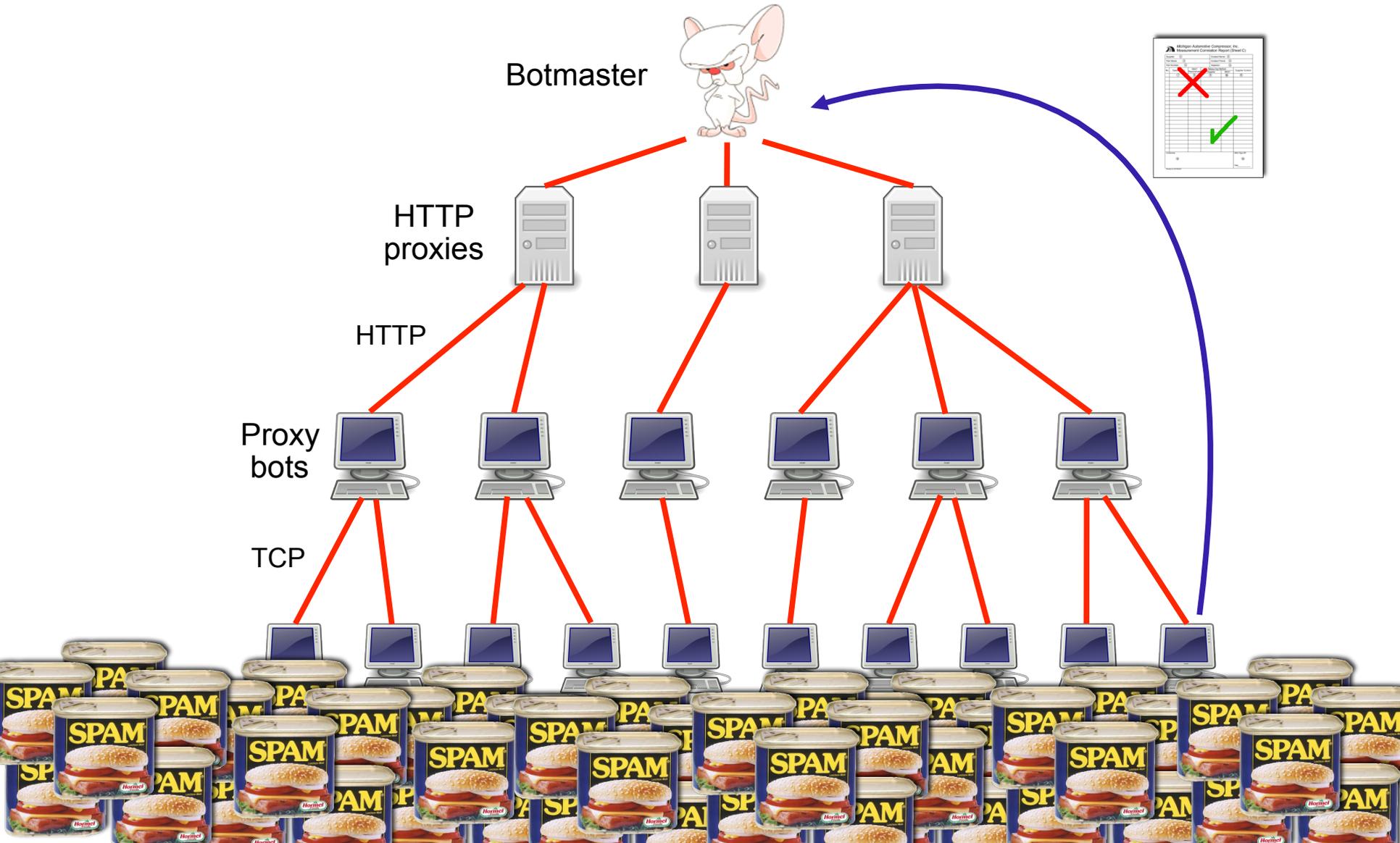
Figure 2: Snippet of a spam template, showing the transformation of an email header from template (top) to resulting content (bottom). The ▷-symbol indicates line continuations. Bold text corresponds to the formatting macros and their evaluation.

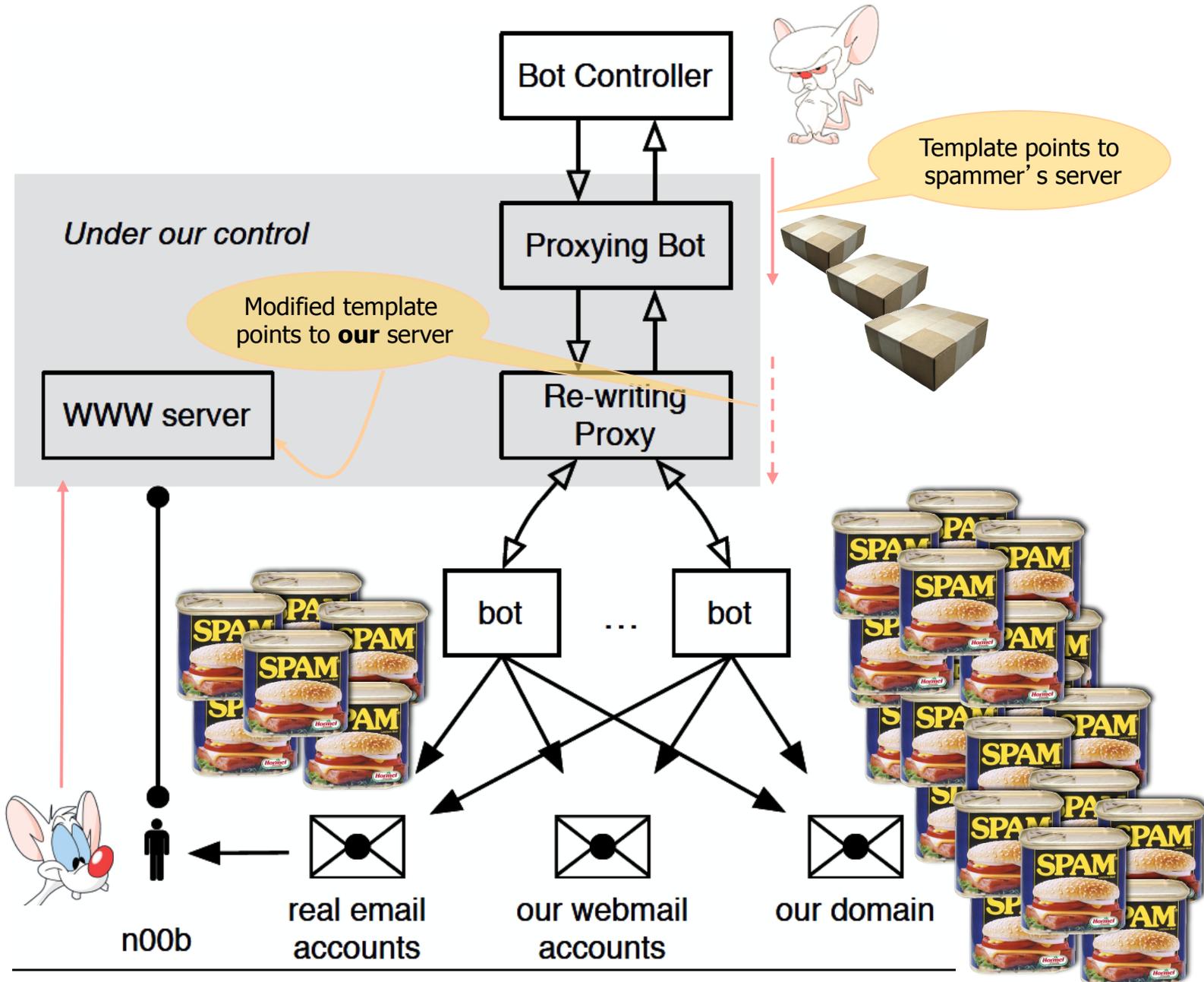
Synthetic diversity aims to thwart content-based anti-spam filtering

MACRO	SEEN LIVE	FUNCTIONALITY
(O)	✓	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.
(Cnum)	✓	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.
(Fstring)	✓	Random value from the dictionary named <i>string</i> . ²
(Gstring)	✓	Line-wrap <i>string</i> into 72 characters per line.
(Hstring)		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.
(Jstring)		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.
(Ostring:num)	✓	Randomized message identifier element compatible with Microsoft SMTPSVC.
(Pnum ₁ [-num ₂]:string)	✓	Random string of num ₁ (up to num ₂ , if provided) characters taken from <i>string</i> .
(Qstring)		Quoted-printable “=” linewrapping.
(Rnum ₁ -num ₂)	✓	Random number between num ₁ and num ₂ . Note, special-cased when used with (D).
(Ustring)		Randomized percent-encoding of <i>string</i> .
(Vnum)	✓	Inserts the value of the field identified by (Cnum).
(W)		Time and date as plain numbers, e.g. “20080225190434”.
(X)		Previously selected member of the “names” dictionary.
(Ynum)	✓	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: Reporting





Axiom of Criminal Laziness

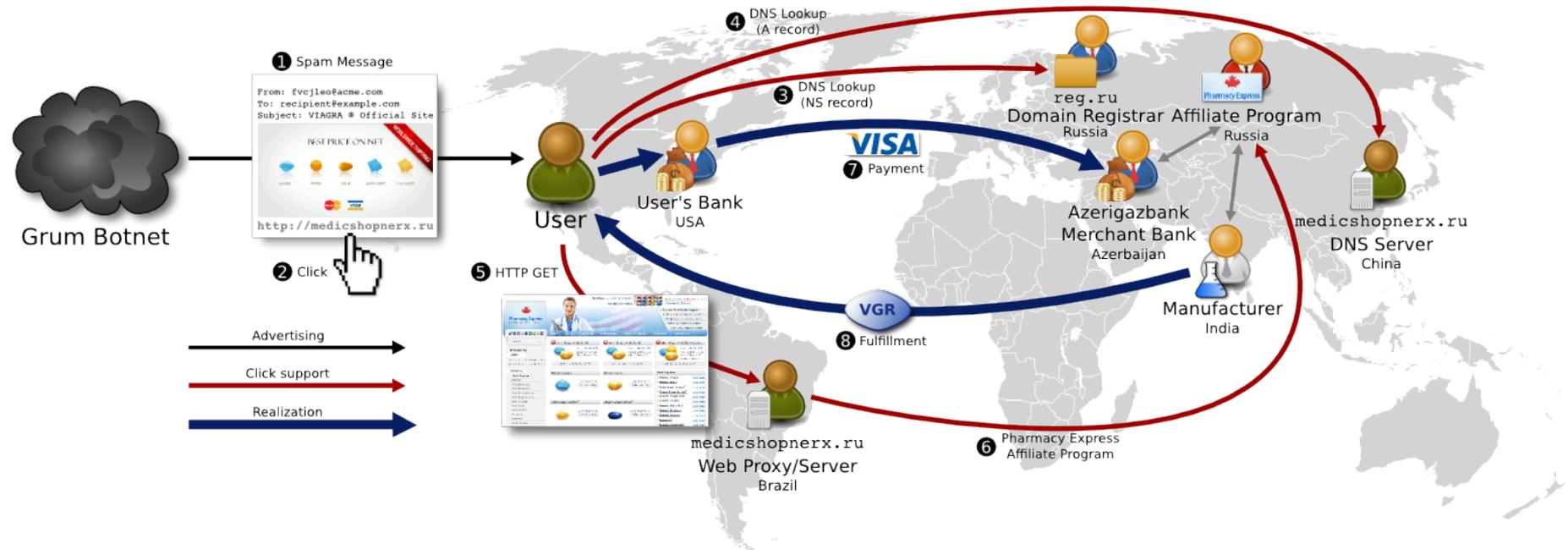
Axiom* of Criminal Laziness

Cybercrooks will **work energetically** to sustain their current cash flow ...

... but **will not look out strategically** beyond it to serve their long-term interests

(* This is a working hypothesis to explain the observed pace of attacker innovation – not something definitively established)

Phases of the Spam Value Chain



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”** ?



Главная

Регистрация

FAQ

Топ10

Саппорт



Логин

Пароль

помнить меня

[забыли пароль?](#)

Войти

60-70%

От дохода

Наши преимущества

- Лучший выхлоп среди аналогичных решений
- Стабильные выплаты
- Надежность сотрудничества
- Индивидуальный подход
- Дружественный саппорт

3-5%

С рефералов

Дополнительная информация

Успешно конвертируем следующие страны: US, CA, AU, GB, DE, FR. Увеличена долгосрочность работы и выхлоп с каждого инсталла. Мы готовы предложить индивидуальные рейты и условия оплаты постоянным партнерам. Вы можете использовать собственные

Новости

29-10-2009

Лендинг

Лендинги на новом домене ожидают ваш траф)

02-10-2009

Обновление модуля

Обновлен билд модуля, улучшен отстук и совместимость с некоторыми лоадерами. Качайте новую версию

14-09-2009



Главная

Registration

FAQ

Top10

A support

ru



Login

Password

remember me

[Forgot your password?](#)

Войти

60-70%

Of revenue

Our advantages

- Best exhaust of similar solutions
- stable payments
- Reliability cooperation
- Individual approach
- friendly support service

3-5%

With referrals

Additional information

Successfully convert the following countries: US, CA, AU, GB, DE, FR. Increased long-term performance and exhaust from each installs. We offer individual and payment rates the constant partners. You can use your own Landing drain web traffic

News

08.05.2010

Happy Holidays!

Dear webmaster! We congratulate you on the Day of Victory! Today osobnenno German installs go well ;)

05/05/2010

Access to auto-update

Dear webmaster! To improve the stability of the affiliate program and prevent discharges of our module access Autoupdate temporarily closed



CASH PARADISE UNIVERSITY

ТВОЙ КЛЮЧ К БОГАТСТВУ

YOUR KEY TO WEALTH



ICQ 24-77777777

JABBER: [REDACTED]



[MAIN](#)

[STUDY PROGRAMS](#)

[RULES](#)

[CONTACT US](#)

Study programs: