Perspectives on Countering Internet Attacks and Disrupting Their Ecosystem

Vern Paxson

EECS, University of California, Berkeley

International Computer Science Institute (ICSI)

vern@eecs.berkeley.edu

June 4, 2012

Overview

- Traditional technical perspective: detecting & blocking Internet attacks
  - Filtered through the lens of network-based monitoring
  - Pitfalls, challenges & trends

- New perspective: cybercrime economics
  - Vast majority of modern attacks motivated by making money
  - Maybe the most effective way to counter attacks is to *render them unprofitable*

Nature of Network-Based Security Monitoring

- Idea: watch network activity to detect problems, intercede to prevent/limit
- Fundamental appeal: cheap & easy-to-secure
- Drawback #1: **bolt-on** / **reactive**
  - Solutions often lack completeness / coherence
  - Greatly increases evasion opportunities
- Drawback #2: **limited visibility**
  - Monitoring internal enterprise traffic or inter-VM traffic requires pervasive deployment
  - Intractability of analyzing complex appl. semantics
  - Blind* to *encrypted* traffic

Pitfalls in Detecting/Blocking Attacks

- Challenge #1: coming to the domain from another discipline
  - Due to domain's rapid innovation, very easy to underestimate evolution/relevance
- **Machine learning** pitfall: *failure to illuminate*
- **Hardware pitfall**: focusing on packet *signatures*
  - Rather than application analysis
- **Modeling pitfall**: focus on tractability rather than relevance (= new insight)

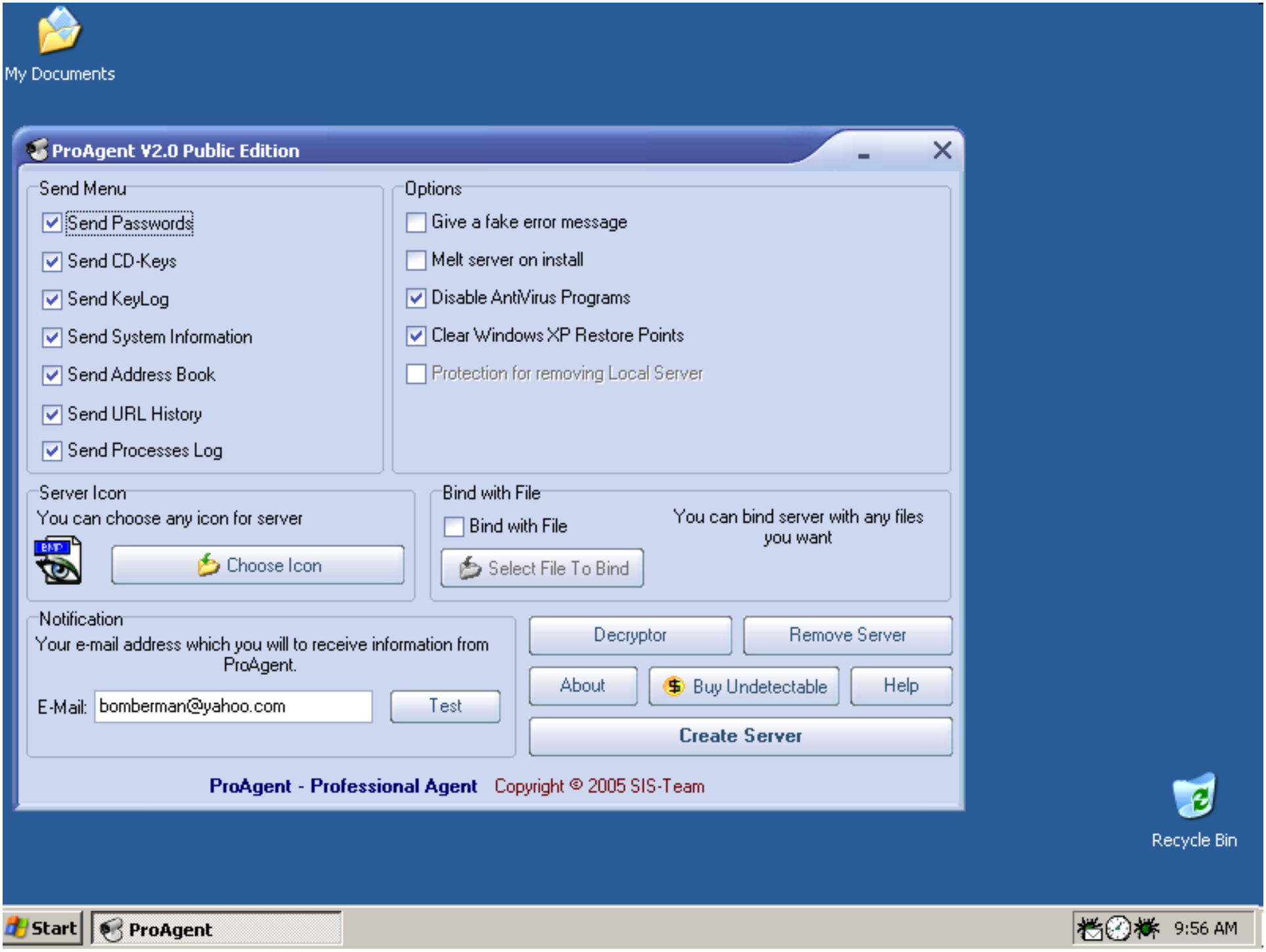
Pitfalls in Detecting/Blocking Attacks, con't

- Challenge #2: resources to fuel analysis
  - Few overt indications that a given resource is lacking
- Data pitfall #1: limited measurements (e.g., Lab)
  - No indication that environment *lacks diversity*
- Data pitfall #2: leveraging public traces / simulation
  - Especially Lincoln Labs and KDD Cup!
- Instead: for data, need access to operational environments and/or large-scale Internet services
  - Can require nurturing special relationships
- Tool pitfall: assuming Snort is *state-of-the-art*
  - Whether it's appropriate requires careful assessment

Pitfalls in Detecting/Blocking Attacks, con't

- Challenge #3: establishing *operational relevance*
  - Will a given approach actually make a difference?
- Need to illuminate false positive/negative tradeoff
  - Need to consider *Base Rate Fallacy*
- Pitfall: failure to illuminate why FP/FNs occur
  - Actionable decisions?
- Pitfall: failure to illuminate why TP/TNs occur!
  - Which components/features matter and which don't?
- Need to illuminate role of (minimal) *parameters*, how to set them, how they do/don't generalize

The Cybercrime Ecosystem

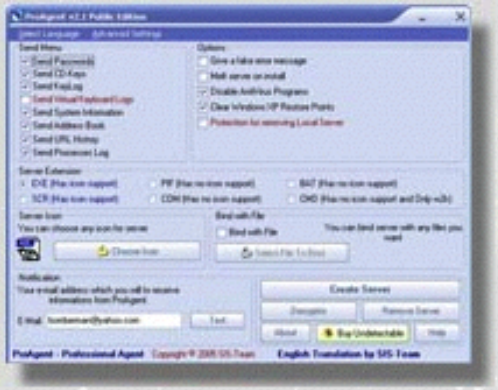

My Documents
ProAgent V2.0 Public Edition
Send Menu
Send Passwords
Send CD-Keys
Send KeyLog
Send System Information
Send Address Book
Send URL History
Send Processes Log
Options
Give a fake error message
Melt server on install
Disable AntiVirus Programs
Clear Windows XP Restore Points
Protection for 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: bomberman@yahoo.com
Test
Decryptor
Remove Server
About
Buy Undetectable
Help
Create Server
ProAgent - Professional Agent
Copyright © 2005 SIS-Team
Recycle Bin
Start
ProAgent
9:56 AM

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

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

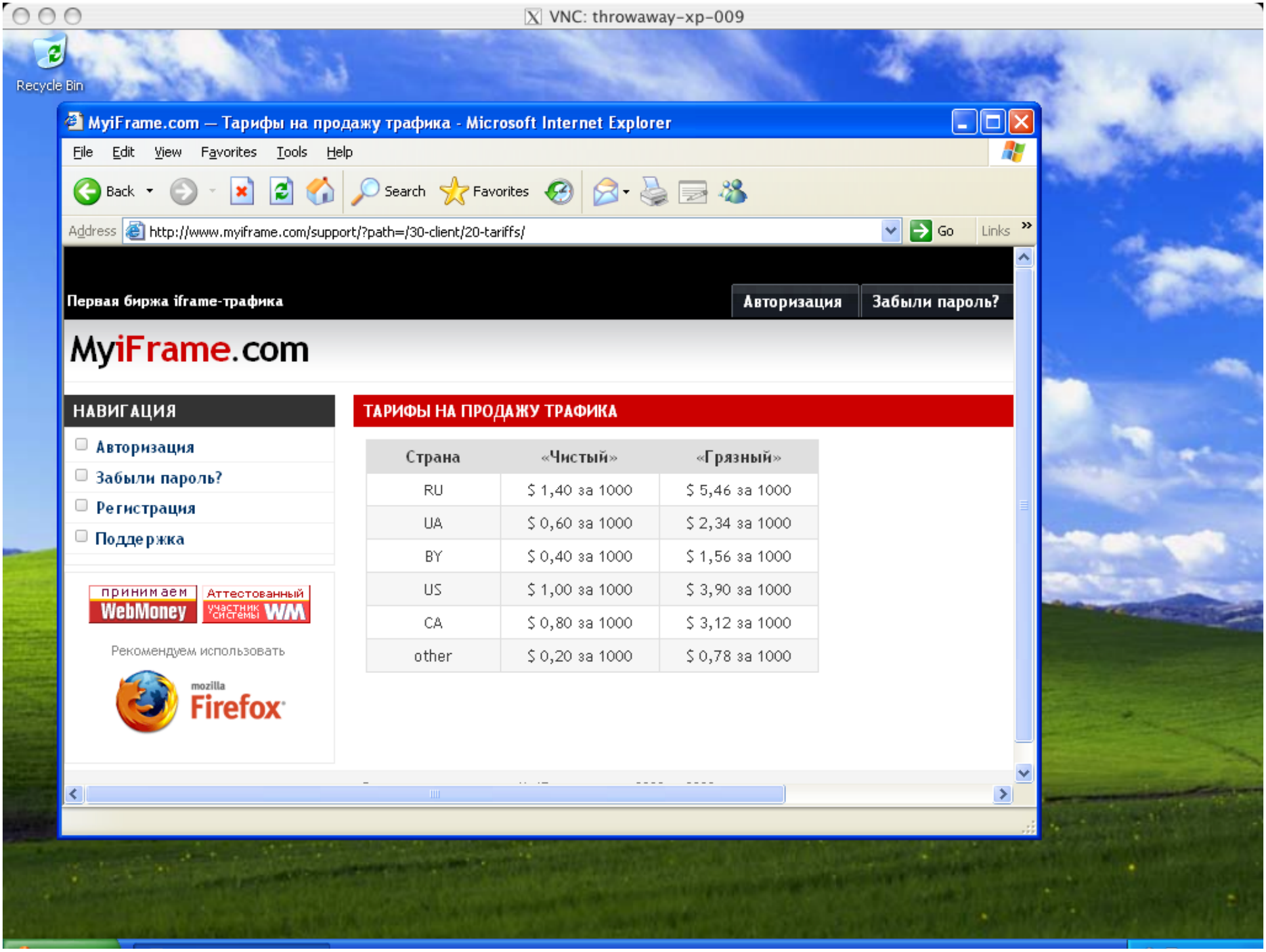
(You Just Need To Type In The CAPTCHAs To Create Accounts)

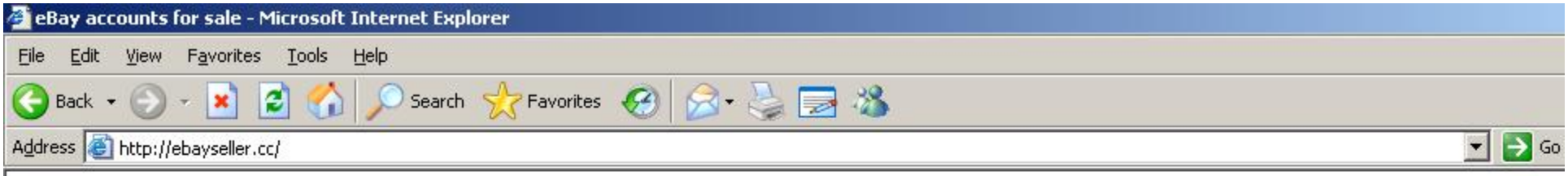
Social Networks			
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager	PayPal Buy Now	~~$180.95~~	$140.00
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)	PayPal Buy Now	~~$360.95~~	$320.00
YouTube Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00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


VNC: throwaway-xp-009
Recycle Bin
MyiFrame.com — Тарифы на продажу трафика - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.myiframe.com/support/?path=/30-client/20-tariffs/
Go Links
Первая биржа iframe-трафика
Авторизация
Забыли пароль?
MyiFrame.com
НАВИГАЦИЯ
Авторизация
Забыли пароль?
Регистрация
Поддержка
принимаем WebMoney
Аттестованный участник системы WM
Рекомендуем использовать
mozilla Firefox
ТАРИФЫ НА ПРОДАЖУ ТРАФИКА
Страна | «Чистый» | «Грязный»
RU | $ 1,40 за 1000 | $ 5,46 за 1000
UA | $ 0,60 за 1000 | $ 2,34 за 1000
BY | $ 0,40 за 1000 | $ 1,56 за 1000
US | $ 1,00 за 1000 | $ 3,90 за 1000
CA | $ 0,80 за 1000 | $ 3,12 за 1000
other | $ 0,20 за 1000 | $ 0,78 за 1000



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$

Welcome to PP24 ! Please use Width Fluid to view full details

You balance is empty, please deposit money to buy paypals

SEARCH PAYPALS

VERIFY (+$0.10)	TYPE (+$0.15)	COUNTRY (+$0.20)	MAIL (+$0.20)	BALANCE (+$0.20)
All Verify	All Type	All Country	☐	☐

SEARCH

AVAILABLE PAYPALS 89

Show 50 entries Search:

PAYPAL EMAIL	VERIFY	TYPE	CARD	BANK	MAIL	BALANCE	FIRST NAME	ADDRESS	COUNTRY	PRICE	
****alksmommy@yahoo.com	Yes	Premier	✓	✓	—	$6.42	Joanna	Panama City	USA	$2.50	☐
****eans123@yahoo.com	Yes	Premier	✓	✓	—	$1.00	Regina	Clifton Park	USA	$2.50	☐
****ibsack@gmail.com	Yes	Premier	✓	✓	—	$121.07	Abigail	Jefferson	USA	$15.00	☐
****ie@gambit.net	Yes	Premier	✓	✓	—	$1,102.37	Gwynn	Tallmadge	USA	$45.00	☐
****l.stevenson@gmail.com	Yes	Premier	✓	✓	—	$209.03	Michal	Galloway	USA	$20.00	☐
****ney_bruesch@yahoo.com	Yes	Premier	✓	✓	—	$18.41	Courtney	Gurnee	USA	$4.00	☐


Installs4Sale.net - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://installs4sale.net/
Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Pr
Search Sidewiki Bookmarks Translate AutoLink
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.
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

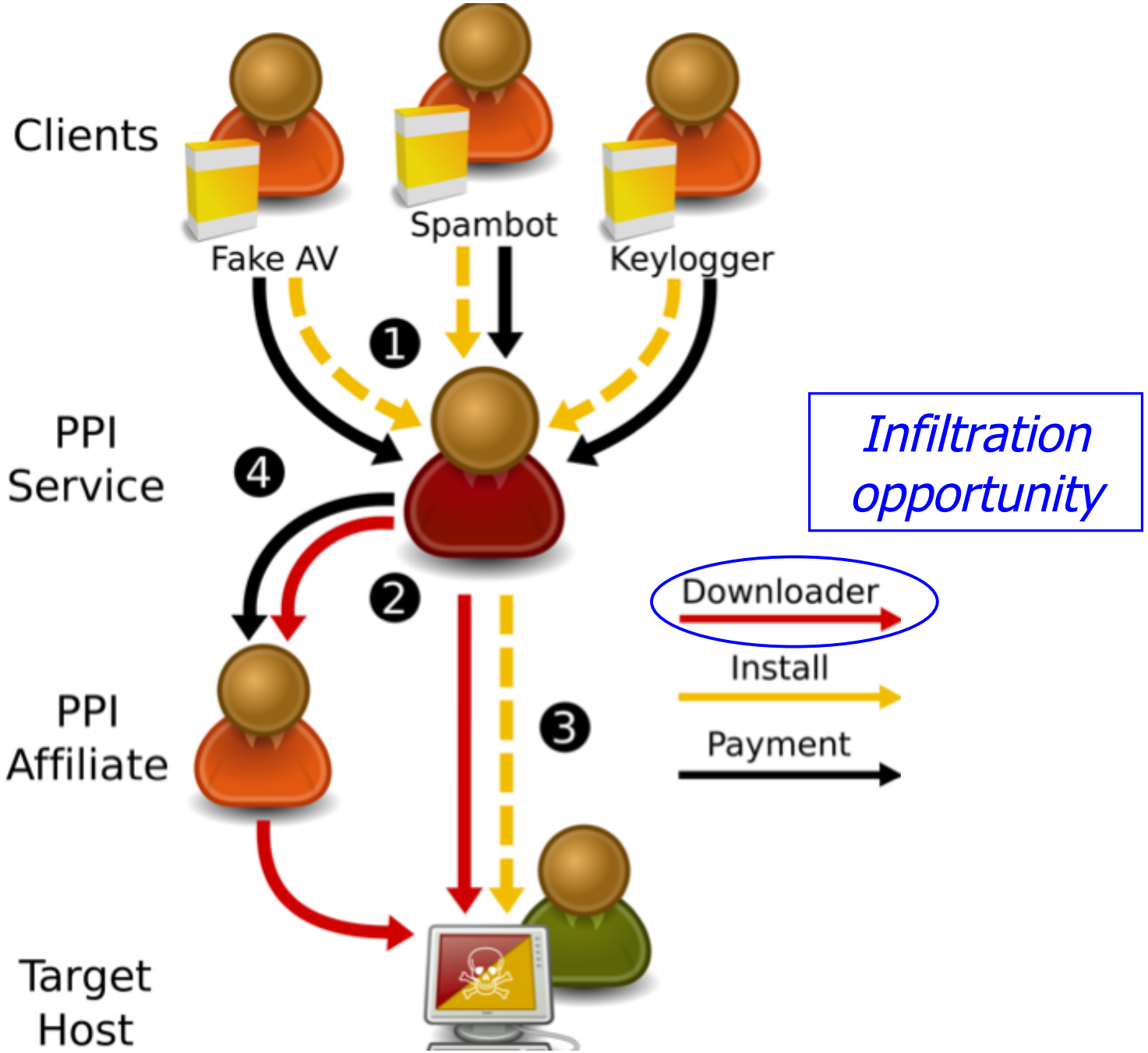
The partnership program «Earning4u» is the easiest way to earn money.
All you need to do to start working with us is register.

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

Key **Features**

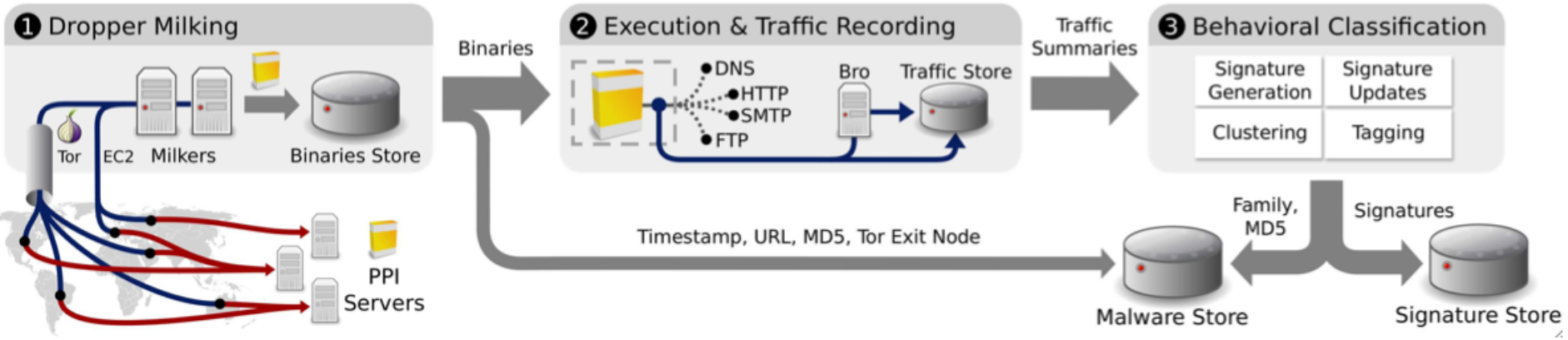
Thanks to an individual approach to each client when you work with our system you have:

- 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


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

Advanced Malware Intelligence via PPI Infiltration

Milking = mimic downloader, repeatedly ask PPI service for next program to install

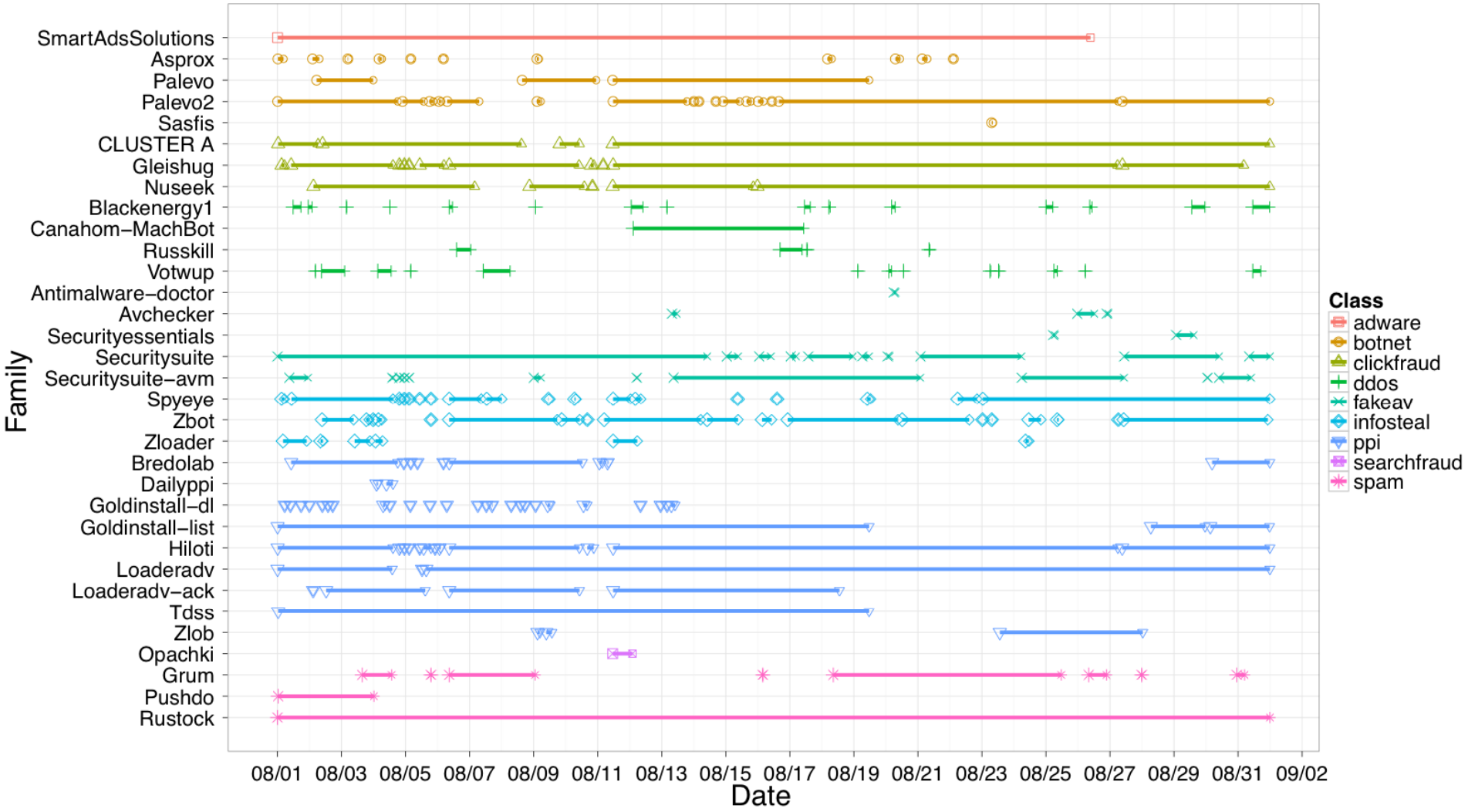


Running since August 2010, we downloaded > 1M binaries (9K distinct) from 4 different affiliate programs

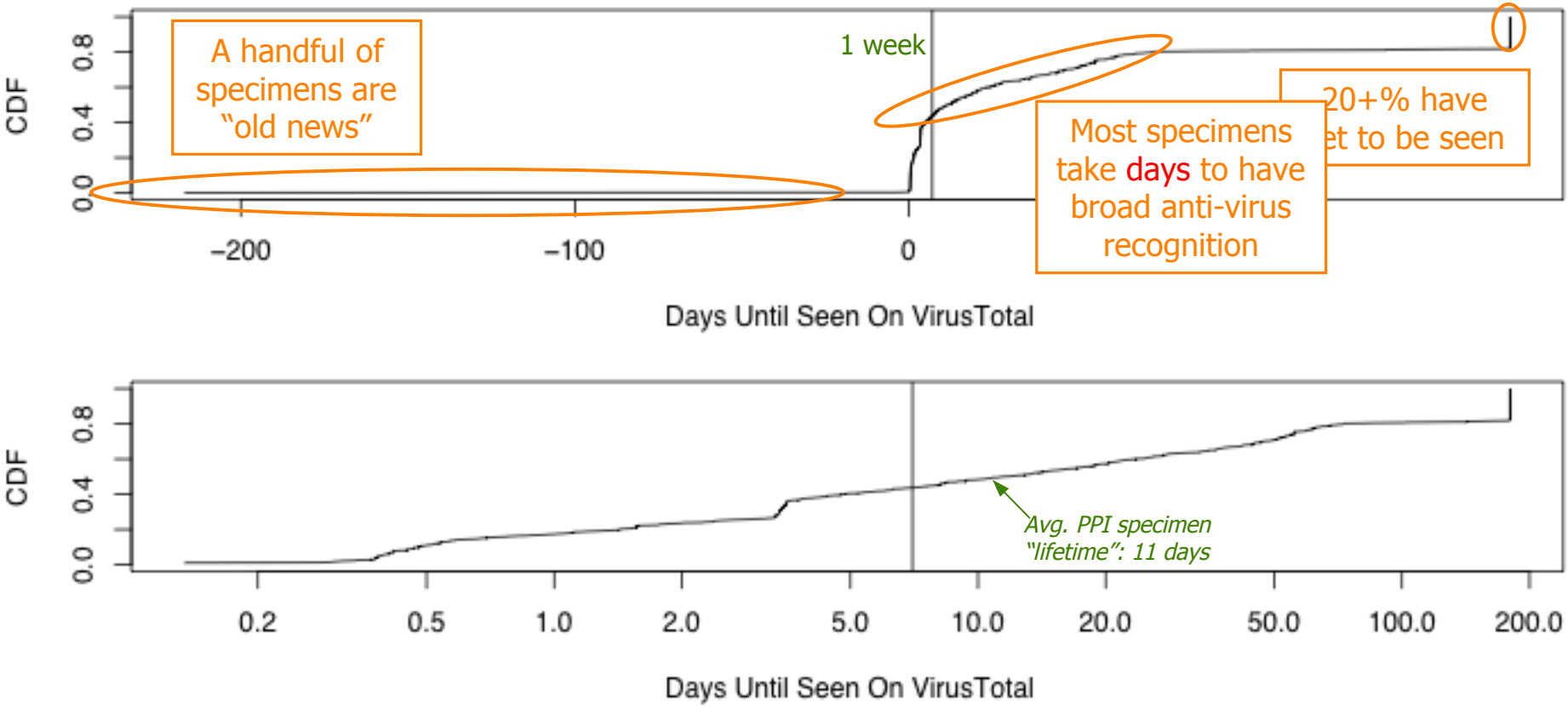
	NAME	%	MONETIZATION	KIT	SEEN
1	Palevo	7.50	DoS,Info stealer	✓	✓
2	Hiloti	4.69	Downloader/PPI		✓
3	Zbot	3.62	Info stealer	✓	✓
4	FakeRean	3.47	Rogue AV(s)		✓
5	Onlinegames	2.94	Info stealer		?
6	Rustock	2.66	Spam		✓
7	Ldpinch	2.64	Info stealer	✓	?
8	Renos	2.58	Rogue AV(s)		?
9	Zlob	2.54	Rogue software		✓
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		

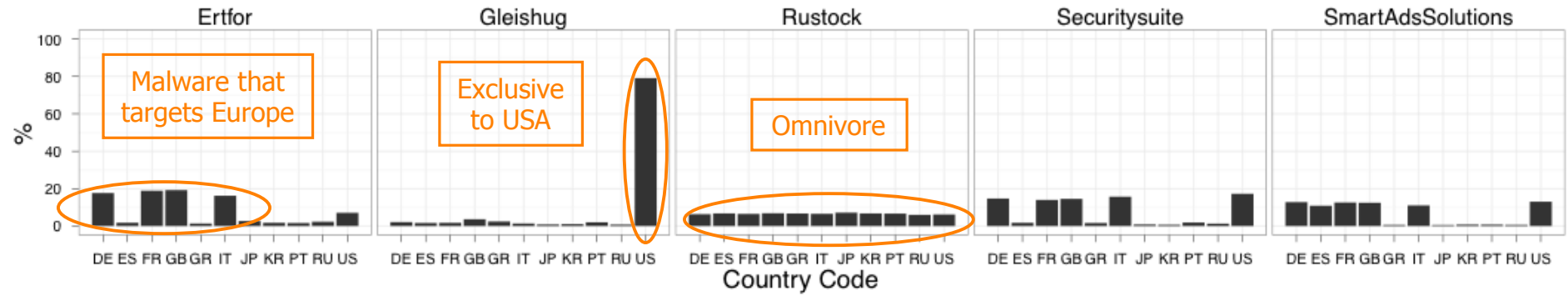
Table 2: FireEye's top 20 malware families observed in their MAX Cloud network on the April–June 2010 time

The majority of the world's top malware appeared in our "milk"



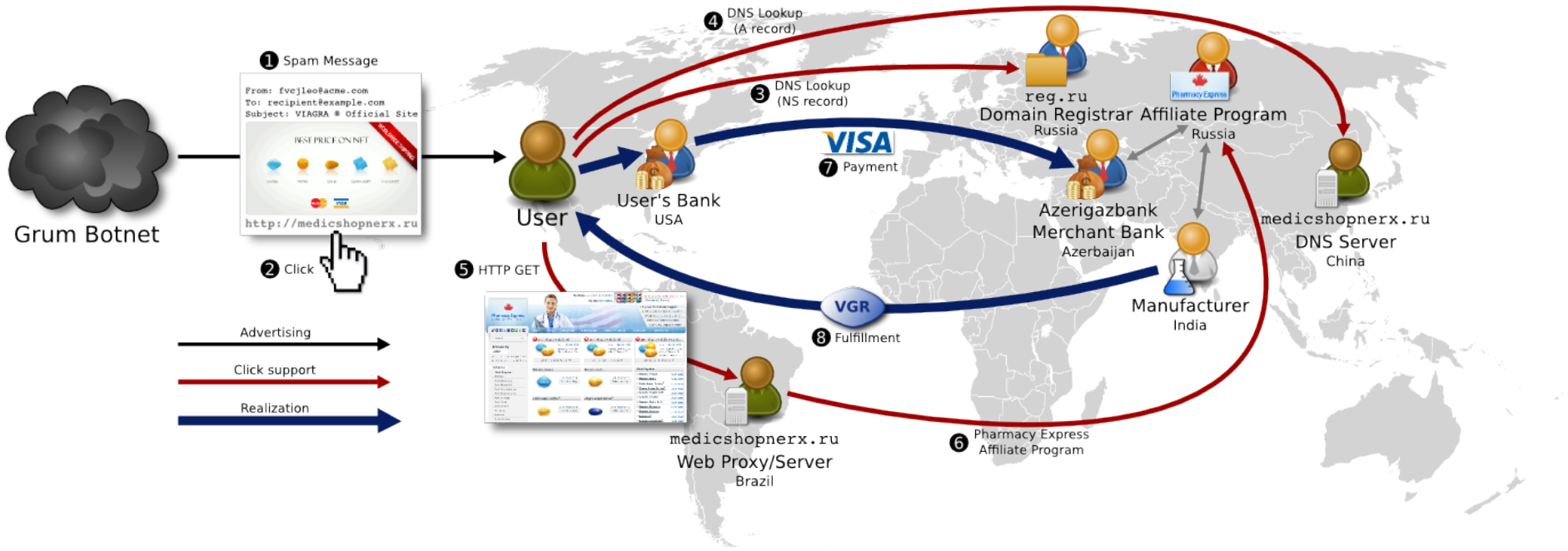
PPI distribution of malware during August 2010


A handful of specimens are "old news"
1 week
20+% have
et to be seen
Most specimens take days to have broad anti-virus recognition
CDF
0.0
0.4
0.8
−200
−100
0
Days Until Seen On VirusTotal
CDF
0.0
0.4
0.8
Avg. PPI specimen "lifetime": 11 days
0.2
0.5
1.0
2.0
5.0
10.0
20.0
50.0
100.0
200.0
Days Until Seen On VirusTotal


Ertfor
Gleishug
Rustock
Securitysuite
SmartAdsSolutions
Malware that targets Europe
Exclusive to USA
Omnivore
%
100
80
60
40
20
0
DE ES FR GB GR IT JP KR PT RU US
Country Code

Making Money

Phases of the Spam Value Chain



Joint work w/ UCSD

What's the most potent point of intervention?

Affiliate Program	URLs	Volume	Domains
RX–Promotion	160,522,026	21.7%	10,586
Mailien	69,961,211	23.57%	14,444
Pharmacy Express	69,959,633	23.57%	14,381
ED Express	1,578	<0.01%	63
ZedCash (Pharma)	42,297,130	18.93%	6,981
Dr. Maxman	32,184,860	13.19%	5,641
Viagrow	5,222,658	3.57%	386
US HealthCare Inc.	3,196,538	1.42%	167
MaxGentleman	1,144,703	0.39%	672
VigREX	426,873	0.31%	39
Stud Extreme	71,104	0.05%	43
ManXtenz	50,394	<0.01%	33
GlavMed	28,313,136	7.84%	2,933
Online Pharmacy	17,266,034	5.07%	2,922
EvaPharmacy	12,798,999	7.91%	11,285
World Pharmacy	10,412,850	5.88%	691
PH Online	2,971,368	2.14%	101
Swiss Apotheke	1,593,532	0.21%	118
HerbalGrowth	265,131	0.19%	17
RX Partners	229,248	0.15%	448
Stimul-cash	157,537	0.07%	50
MAXX Extend	104,201	<0.01%	23
DrugRevenue	51,637	0.05%	122
Ultimate Pharmacy	44,126	0.02%	12
Greenline	25,021	<0.01%	1,766
Virility	23,528	0.01%	9
MediTrust	6,156	<0.01%	24
RX Rev Share	5,690	<0.01%	183
Unknown Program	3,310	<0.01%	1,270
Canadian Pharmacy	1,392	<0.01%	133
RXCash	287	<0.01%	22
Stallion	80	<0.01%	2
Pharma Total	347,053,630	93.74%	54,142

Affiliate Program	URLs	Volume	Domains
Royal Software	2,291,571	1.48%	572
EuroSoft	694,810	0.31%	1,161
Auth. Soft. Resellers	65,918	<0.01%	4,117
OEM Soft Store	19,436	<0.01%	1,367
Soft Sales	93	<0.01%	35
Software Total	3,071,828	1.79%	7,252

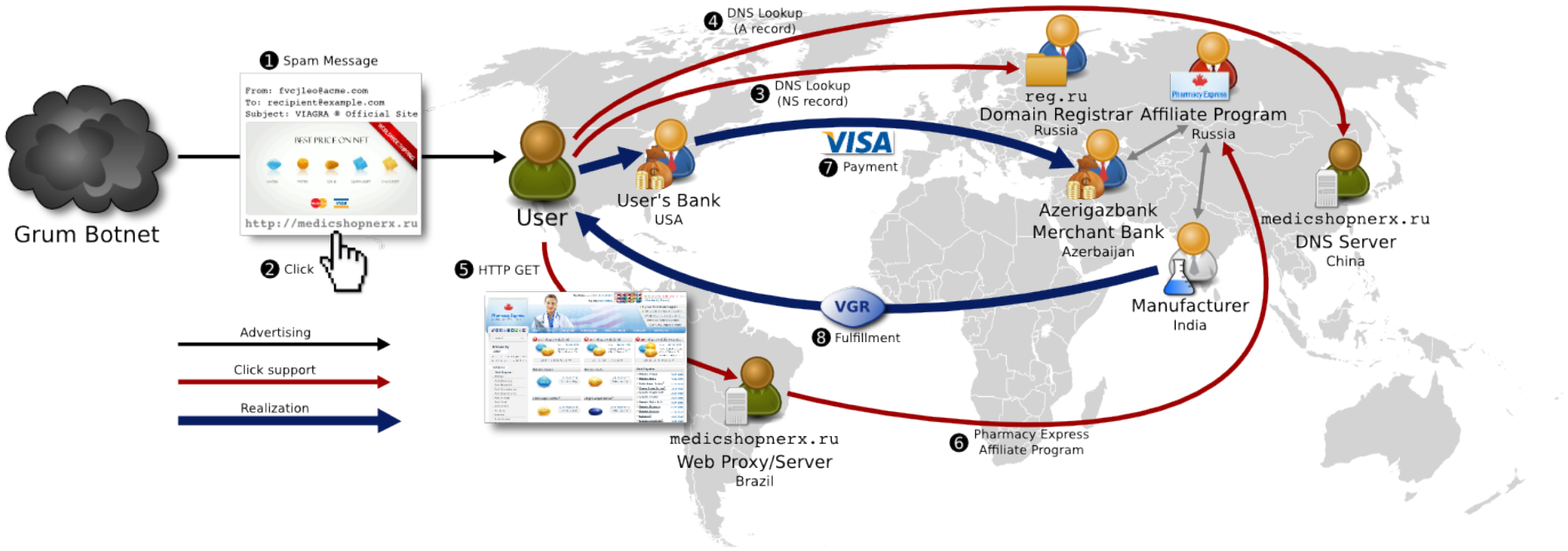
Looked at three categories:

Pharma, Replica, Software

Covered all the major affiliate programs

Affiliate Program	URLs	Volume	Domains
ZedCash (Replica)	13,264,108	4.29%	7,011
Ultimate Replica	10,464,930	3.35%	5,032
Distinction Replica	1,252,816	0.3%	130
Diamond Replicas	506,486	0.14%	1,307
Prestige Replicas	382,964	0.16%	101
Exquisite Replicas	620,642	0.32%	128
One Replica	21,318	0.02%	83
Luxury Replica	11,207	<0.01%	28
Aff. Accessories	3,669	<0.01%	187
Swiss Rep. & Co.	76	<0.01%	15
WatchShop	2,086,930	0.17%	547
Replica Total	15,351,038	4.46%	7,558

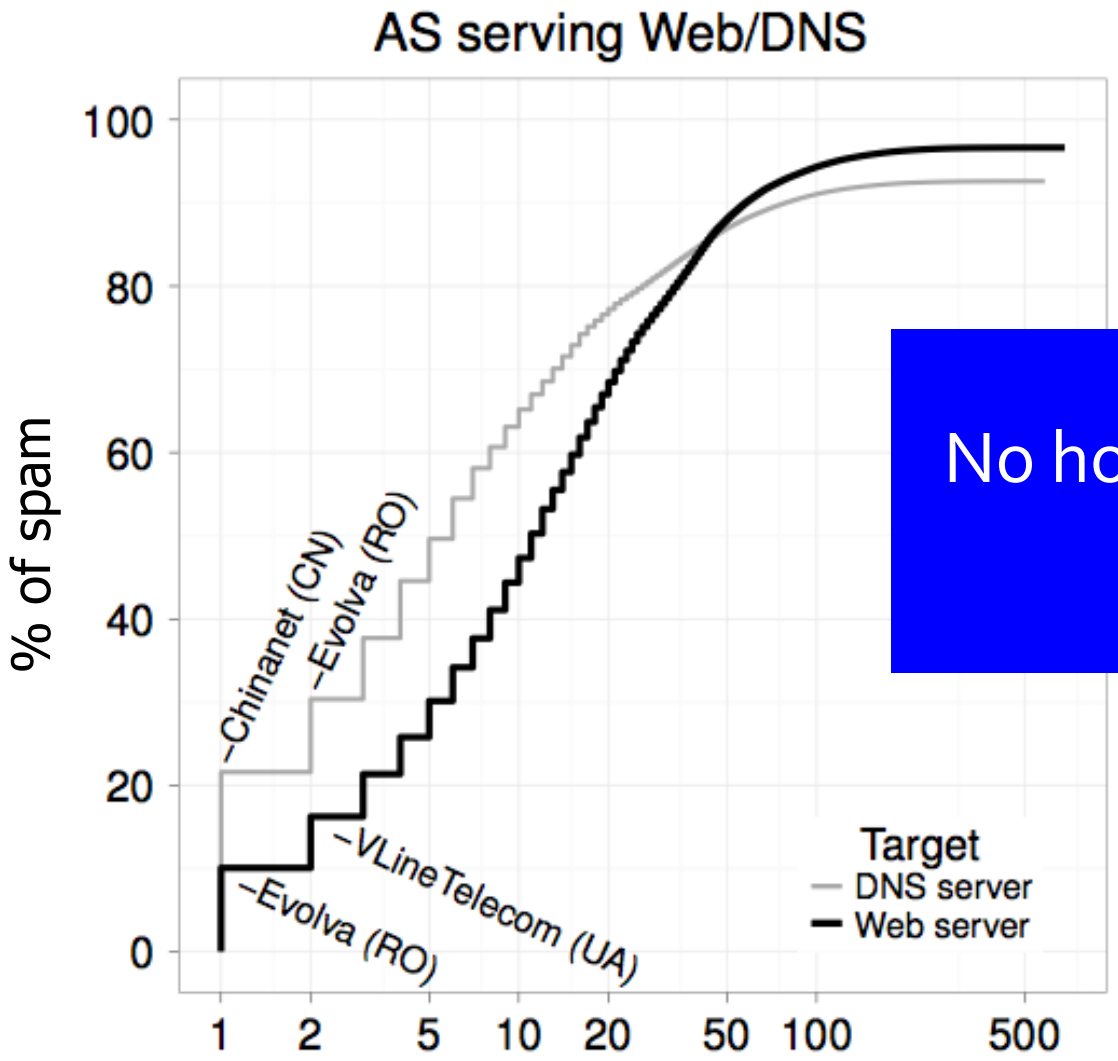
Phases of the Spam Value Chain



Joint work w/ UCSD

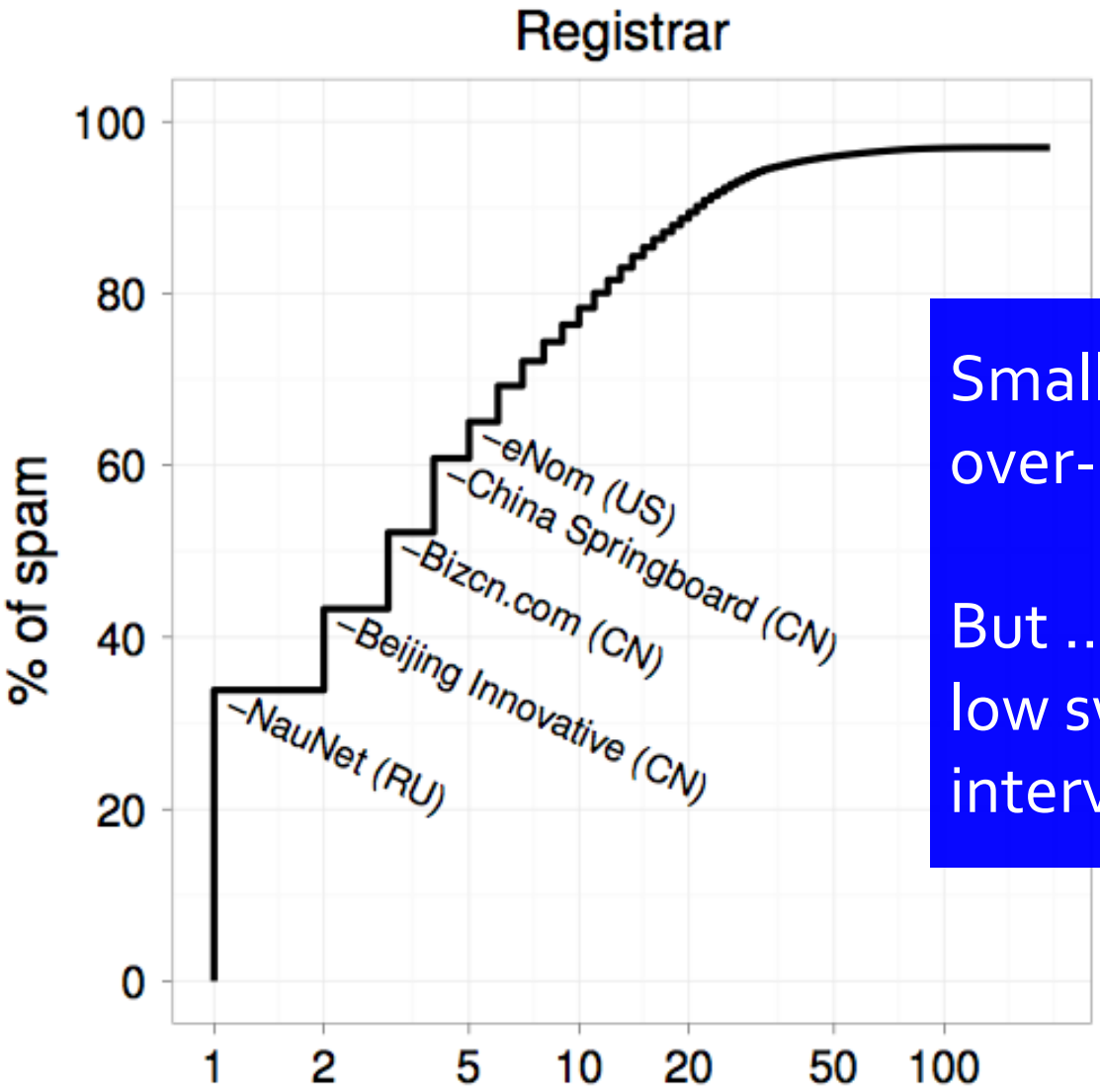
What's the most potent point of intervention?

Hosting bottlenecks



No hosting bottleneck -- long tail

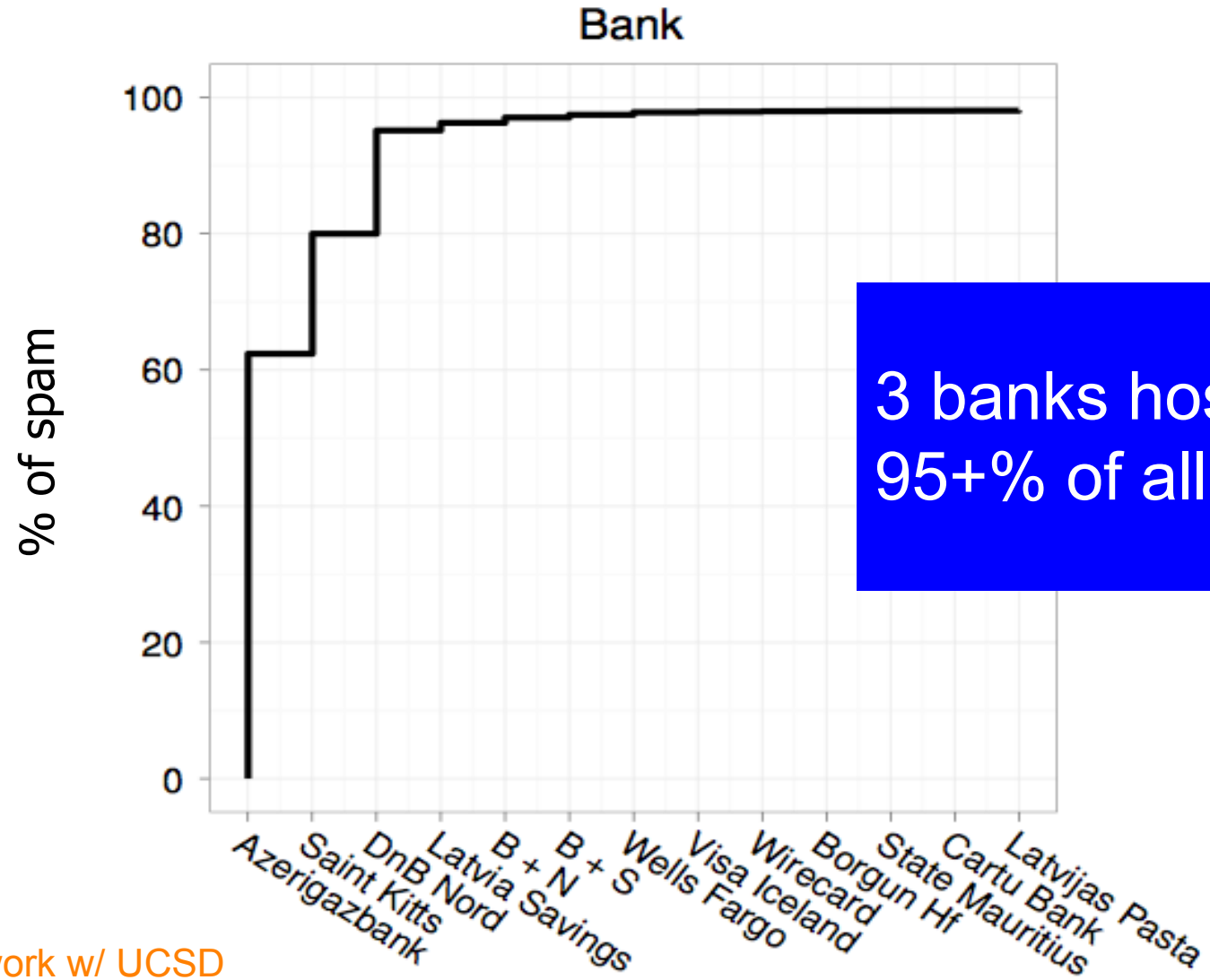
Registrar bottlenecks



Small number of registrars over-represented in spam

But … many alternatives, low switching cost, slow intervention, and long tail

Merchant Bank bottlenecks



3 banks host
95+% of all sales

Joint work w/ UCSD

Summary

- Data = **Gold**
  - From operational environments
  - From large-scale Internet services
  - Can require *nurturing special relationships*
- For detection/defenses, above all we seek ***illumination***
  - Regarding both limitations and simply why something works when it does
  - How will it work in other/different contexts?
- New frontier: *cybercrime ecosystem*
  - Fuels arms-race benefiting other actors, too
  - Just how does profiting from Internet attacks work?
    - And how is it vulnerable to *disruption?*