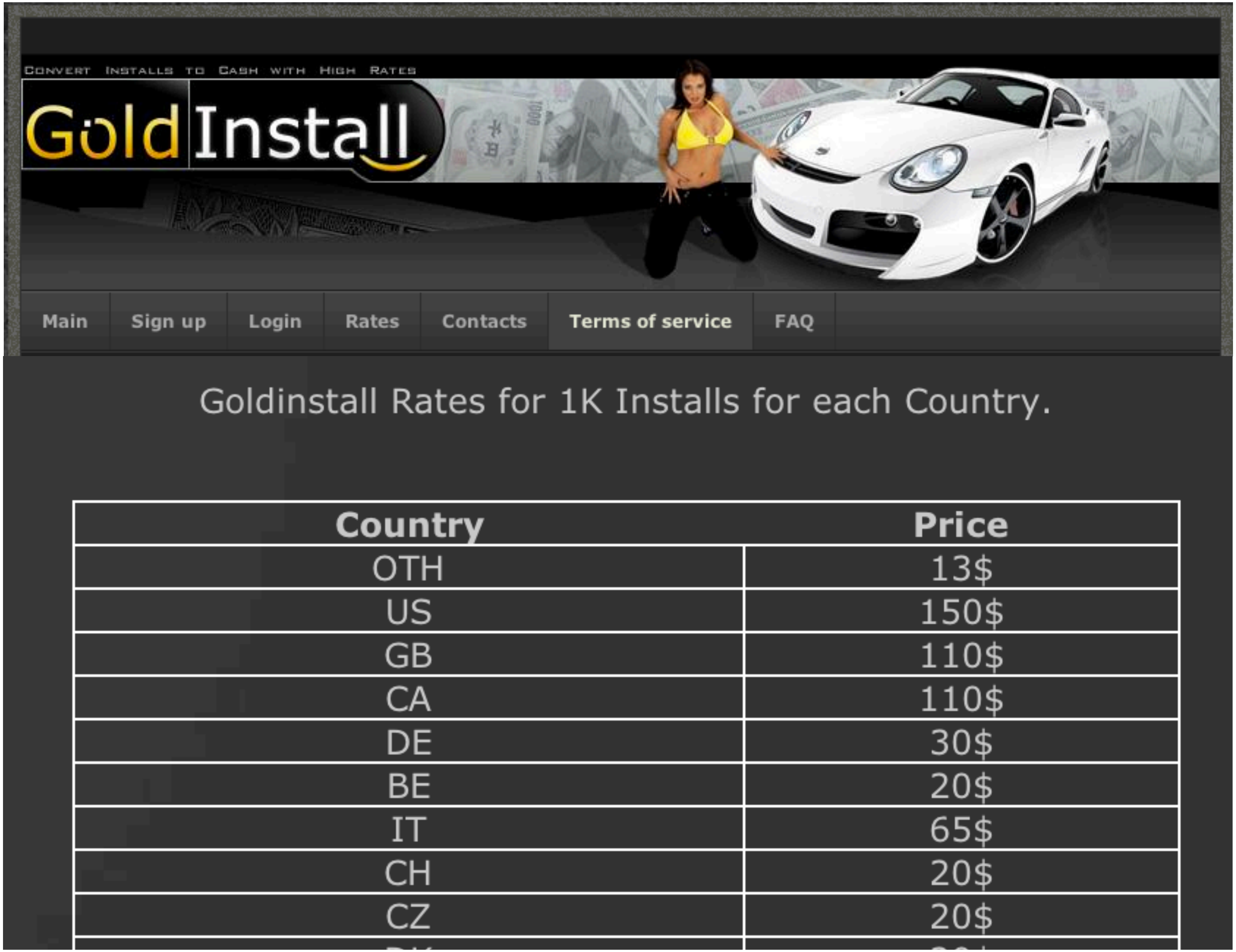
Measuring Pay-Per-Install: The Commoditization of Malware Distribution

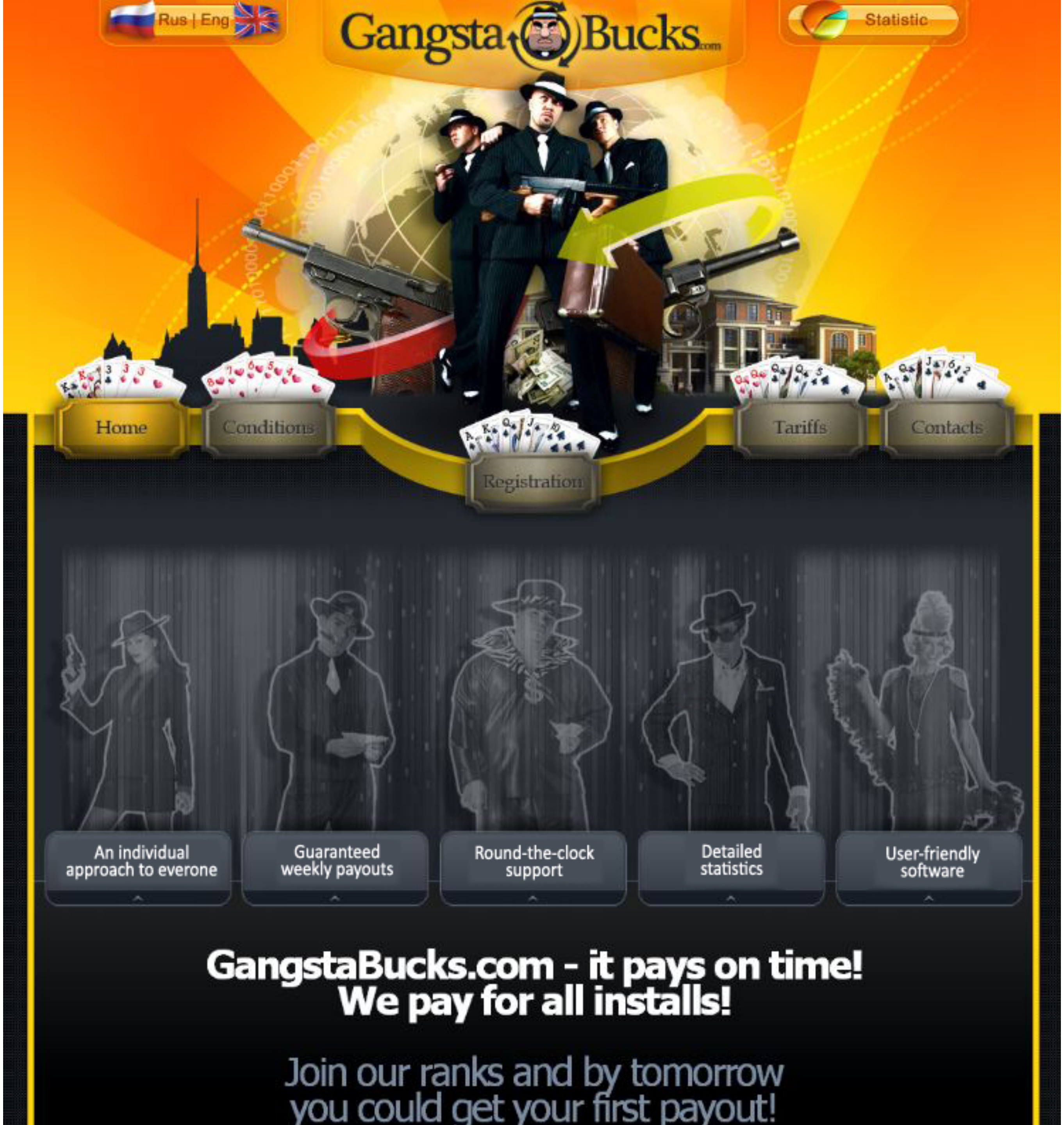
Juan Caballero, **Chris Grier**,
Christian Kreibich and Vern Paxson

IMDEA Software Institute, UC Berkeley,
International Computer Science Institute



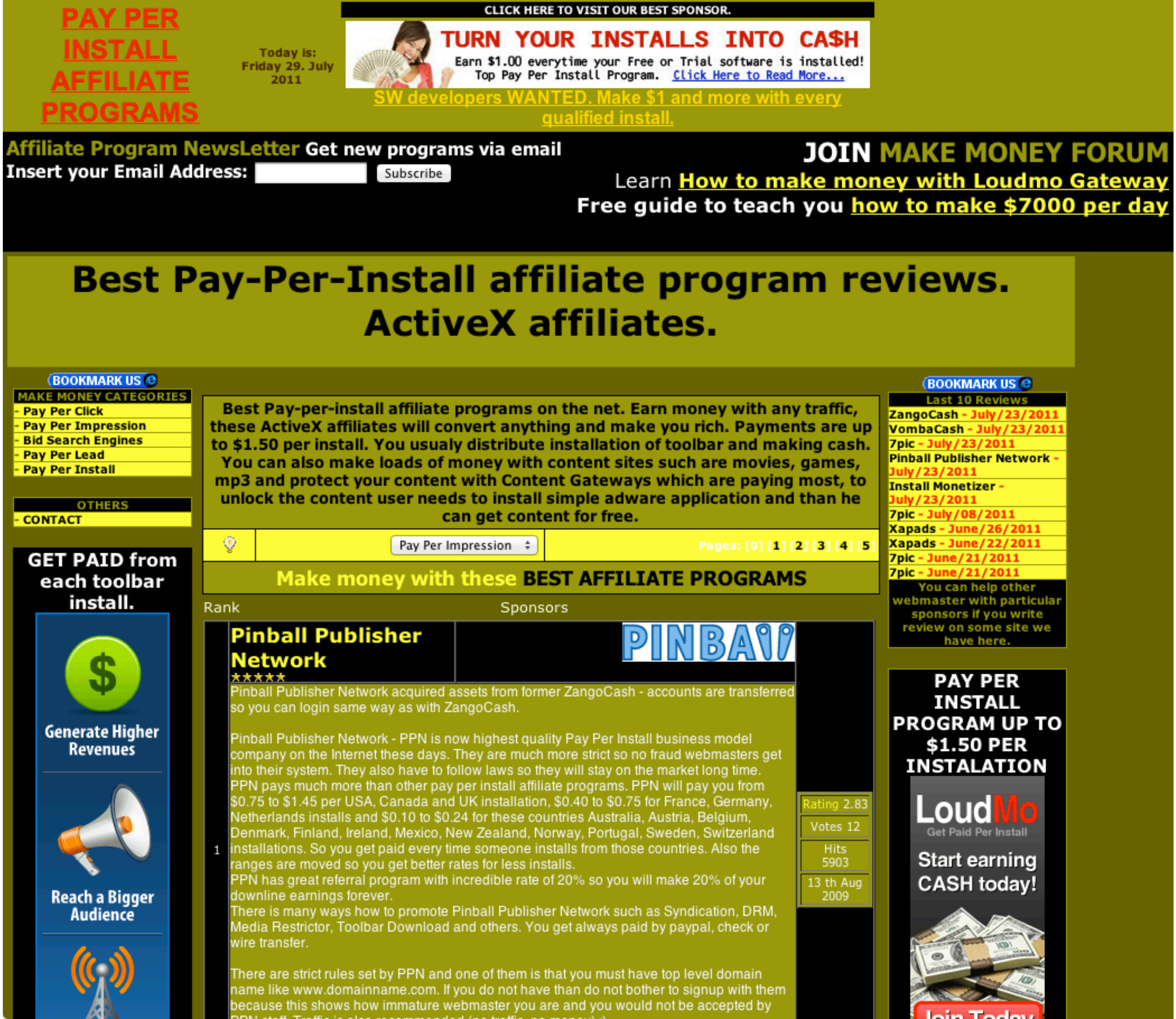
Goldinstall Rates for 1K Installs for each Country.

Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$
IT	65$
CH	20$
CZ	20$



**GangstaBucks.com - it pays on time!
We pay for all installs!**

Join our ranks and by tomorrow
you could get your first payout!



PAY PER INSTALL AFFILIATE PROGRAMS

Today is: Friday 29. July 2011

CLICK HERE TO VISIT OUR BEST SPONSOR.

TURN YOUR INSTALLS INTO CA$H

Earn $1.00 everytime your Free or Trial software is installed! Top Pay Per Install Program. Click Here to Read More...

SW developers WANTED. Make $1 and more with every qualified install.

Affiliate Program NewsLetter Get new programs via email

Insert your Email Address: Subscribe

JOIN MAKE MONEY FORUM

Learn How to make money with Loudmo 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.

Generate Higher Revenues

Reach a Bigger Audience

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.

Pay Per Impression

Pages: [0] [1] [2] [3] [4] [5]

Make money with these BEST AFFILIATE PROGRAMS

Rank Sponsors

Pinball Publisher Network

★★★★★

PINBALL

Pinball Publisher Network acquired assets from former ZangoCash - accounts are transferred so you can login same way as with ZangoCash.

Pinball Publisher Network - PPN is now highest quality Pay Per Install business model company on the Internet these days. They are much more strict so no fraud webmasters get into their system. They also have to follow laws so they will stay on the market long time. PPN pays much more than other pay per install affiliate programs. PPN will pay you from $0.75 to $1.45 per USA, Canada and UK installation, $0.40 to $0.75 for France, Germany, Netherlands installs and $0.10 to $0.24 for these countries Australia, Austria, Belgium, Denmark, Finland, Ireland, Mexico, New Zealand, Norway, Portugal, Sweden, Switzerland installations. So you get paid every time someone installs from those countries. Also the ranges are moved so you get better rates for less installs.
PPN has great referral program with incredible rate of 20% so you will make 20% of your downline earnings forever.
There is many ways how to promote Pinball Publisher Network such as Syndication, DRM, Media Restrictor, Toolbar Download and others. You get always paid by paypal, check or wire transfer.

1

There are strict rules set by PPN and one of them is that you must have top level domain name like www.domainname.com. If you do not have than do not bother to signup with them because this shows how immature webmaster you are and you would not be accepted by PPN staff. Traffic is also recommended (no traffic, no money) :)

Rating 2.83

Votes 12

Hits 5903

13 th Aug 2009

BOOKMARK US

Last 10 Reviews

- ZangoCash - July/23/2011
- VombaCash - July/23/2011
- 7pic - July/23/2011
- Pinball Publisher Network - July/23/2011
- Install Monetizer - July/23/2011
- 7pic - July/08/2011
- Xapads - June/26/2011
- Xapads - June/22/2011
- 7pic - June/21/2011
- 7pic - June/21/2011

You can help other webmaster with particular sponsors if you write review on some site we have here.

PAY PER INSTALL PROGRAM UP TO $1.50 PER INSTALATION

LoudMo Get Paid Per Install

Start earning CASH today!

Join Today

Market for Malware Installation

- **Goal: Measure and understand the the pay-per-install ecosystem**

- Our approach:
  - Infiltrate four PPI programs
  - Develop “milkers” to automatically download malware
  - Download, execute, and classify malware being installed

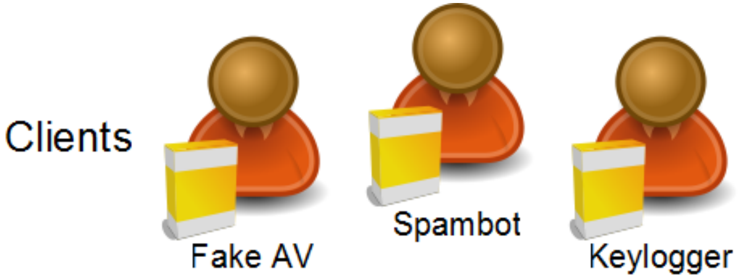
- Insights into the pay-per-install business
  - Real-time monitoring of changes in malware ecosystem
  - Types of clients using PPI
  - Financial impacts of botnet takedown

Outline

- Background on pay-per-install
- Infiltration and monitoring of PPI
- Results and measurements
  - Malware being installed by PPI
  - Repacking of malware
  - Geographically diverse distribution

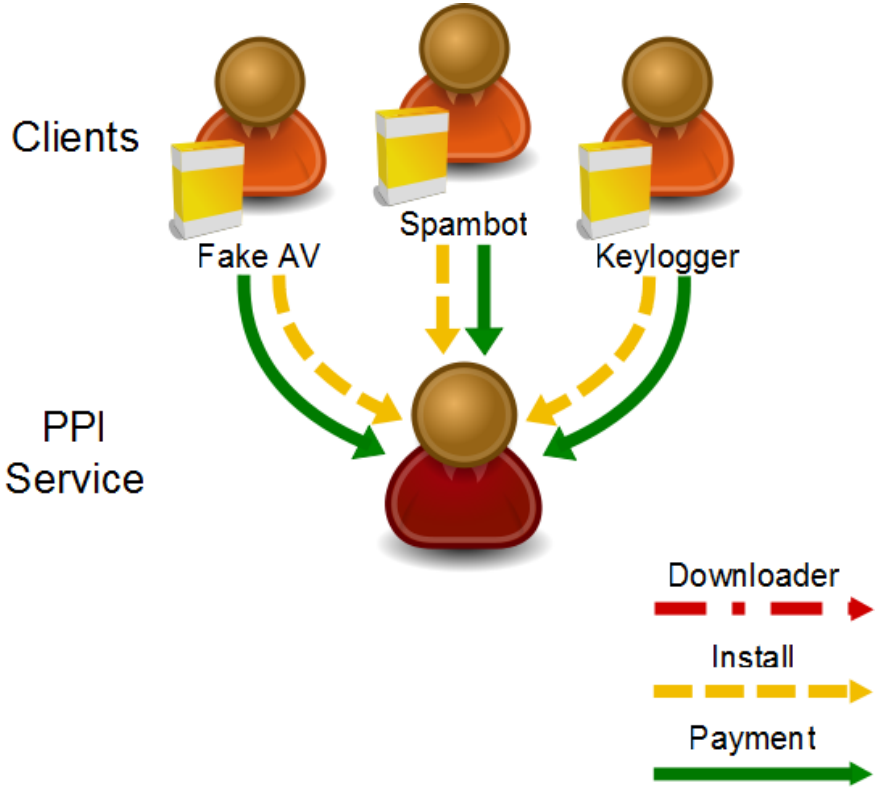
PPI Ecosystem

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



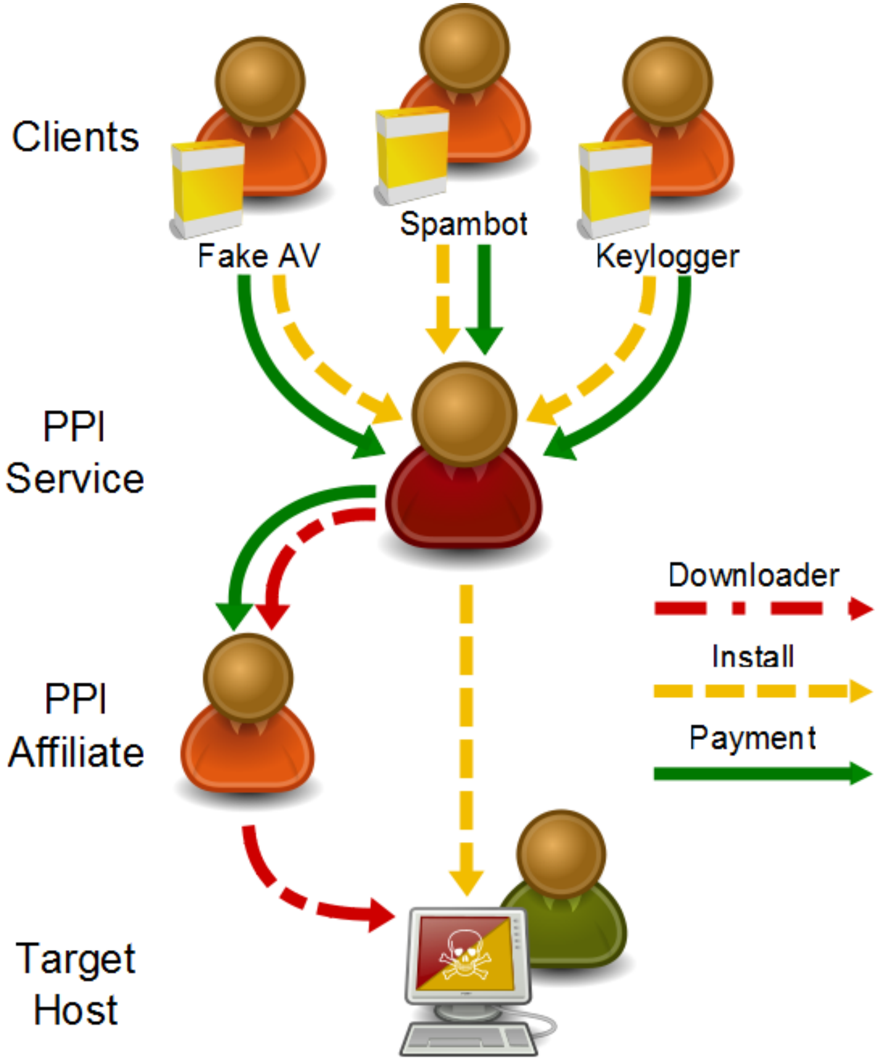
PPI Ecosystem

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

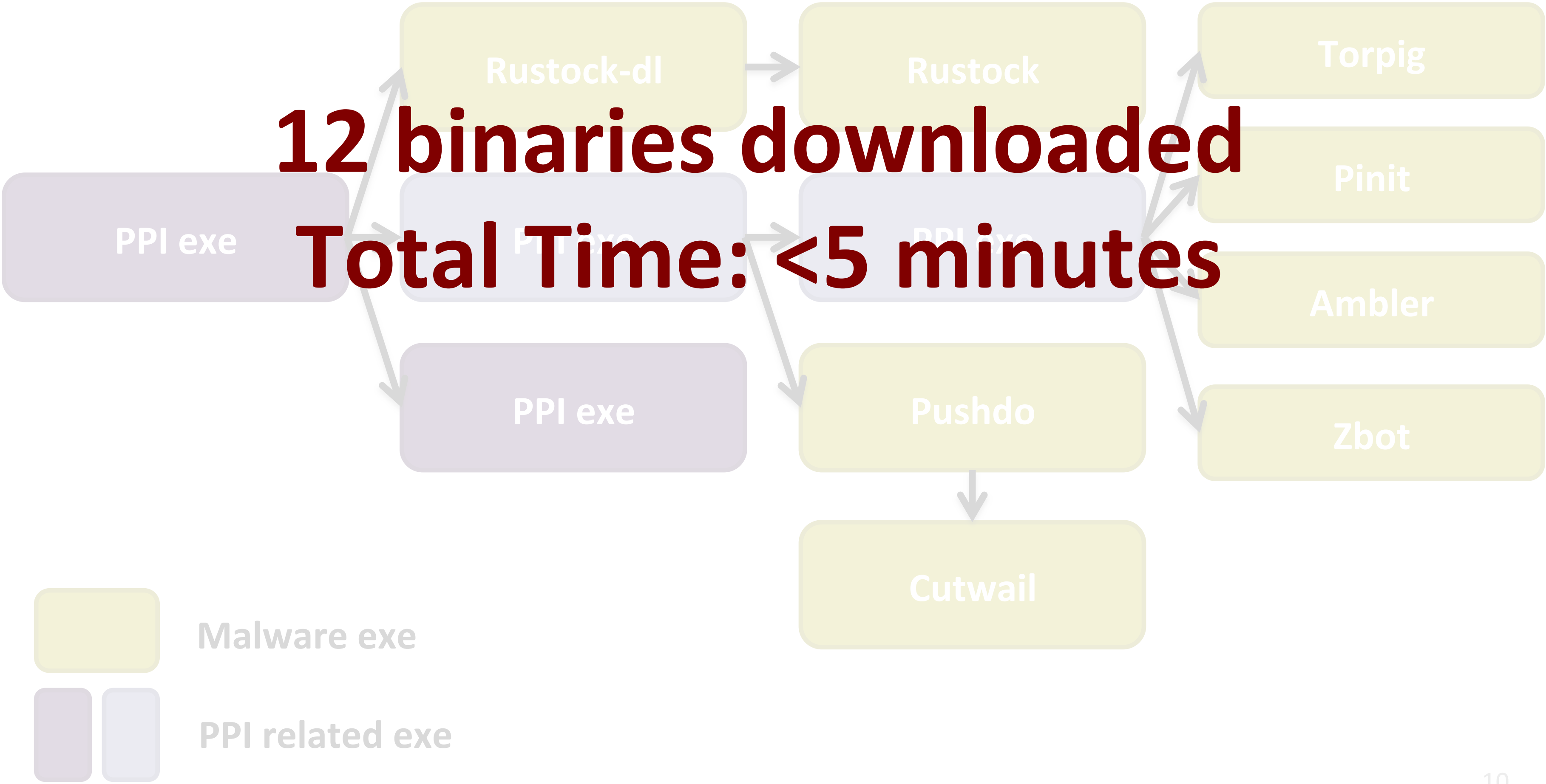


PPI Ecosystem

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



Dropper Lifecycle



12 binaries downloaded

Total Time: <5 minutes

PPI Infiltration and Monitoring

Infiltration Summary

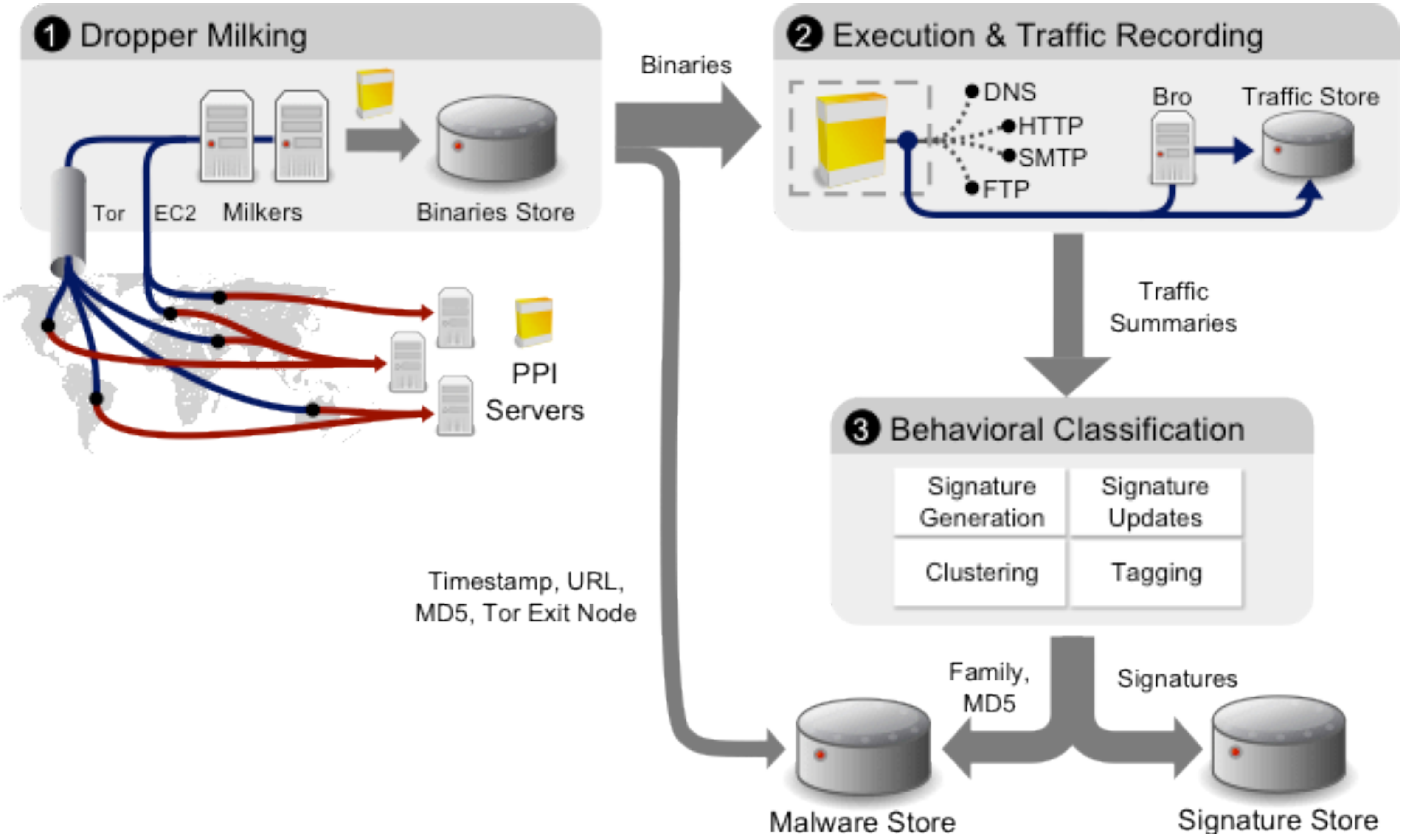
- 12 of the 20 most popular families of malware distributed by PPI services

- Infiltrated four PPI command and control networks
  - Continual monitoring of C&C
  - Download new binaries
  - Download from geo-diverse locations

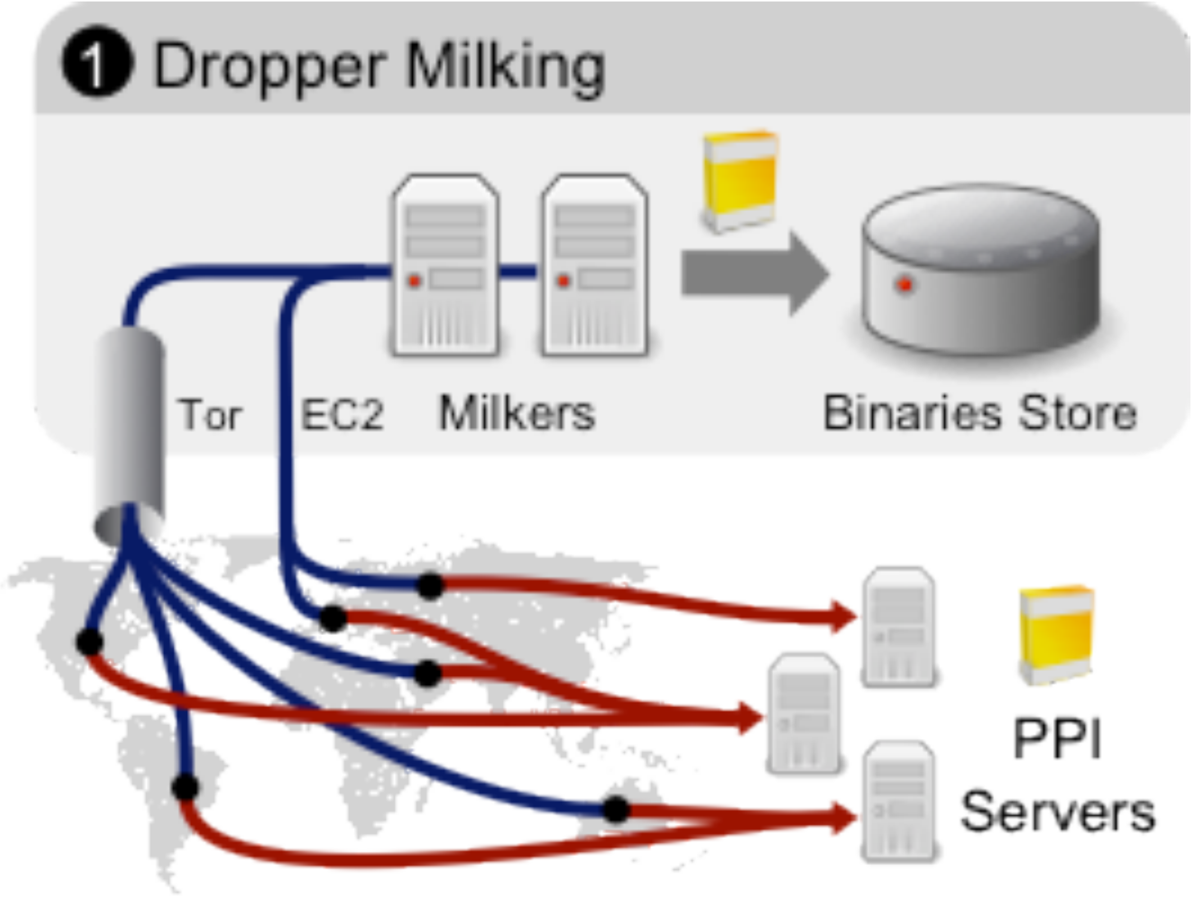
- Dropped Malware
  - 1,060,895 client binaries downloaded
  - 9,153 distinct binaries

World's Top Malware, FireEye, July 2010.
http://blog.fireeye.com/research/2010/07/worlds_top_modern_malware.html

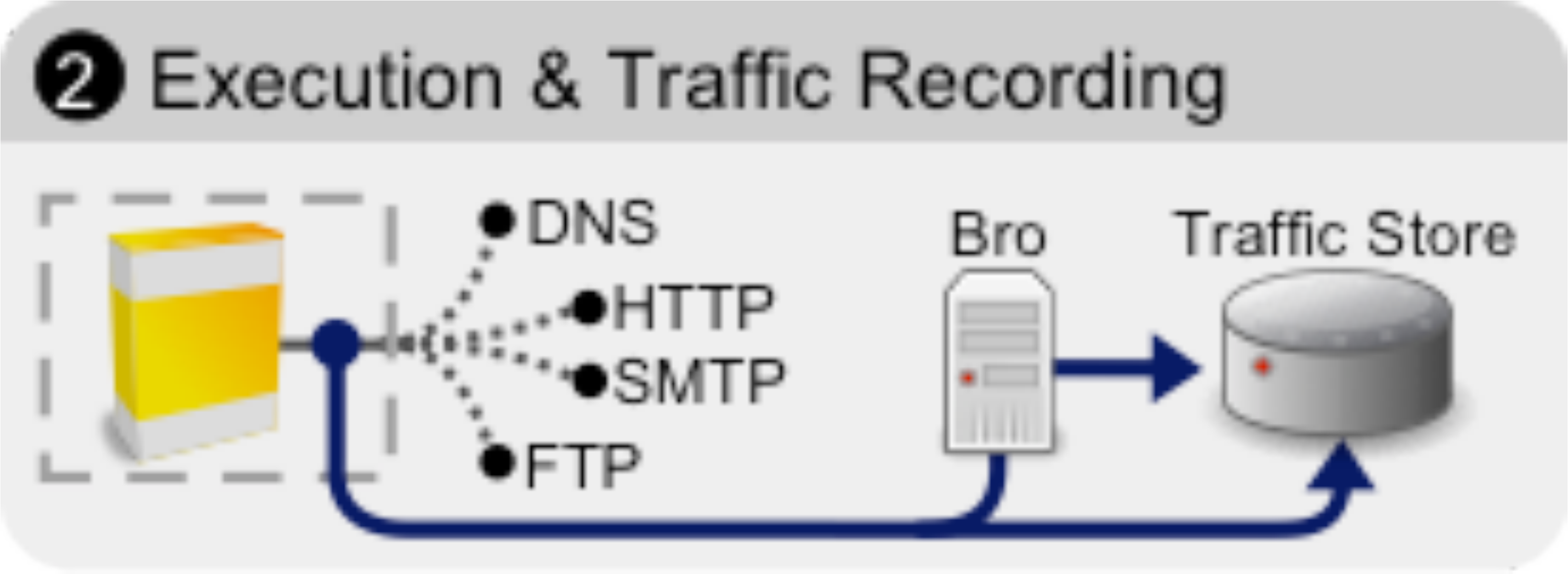
PPI Milking System



Milking PPI Services

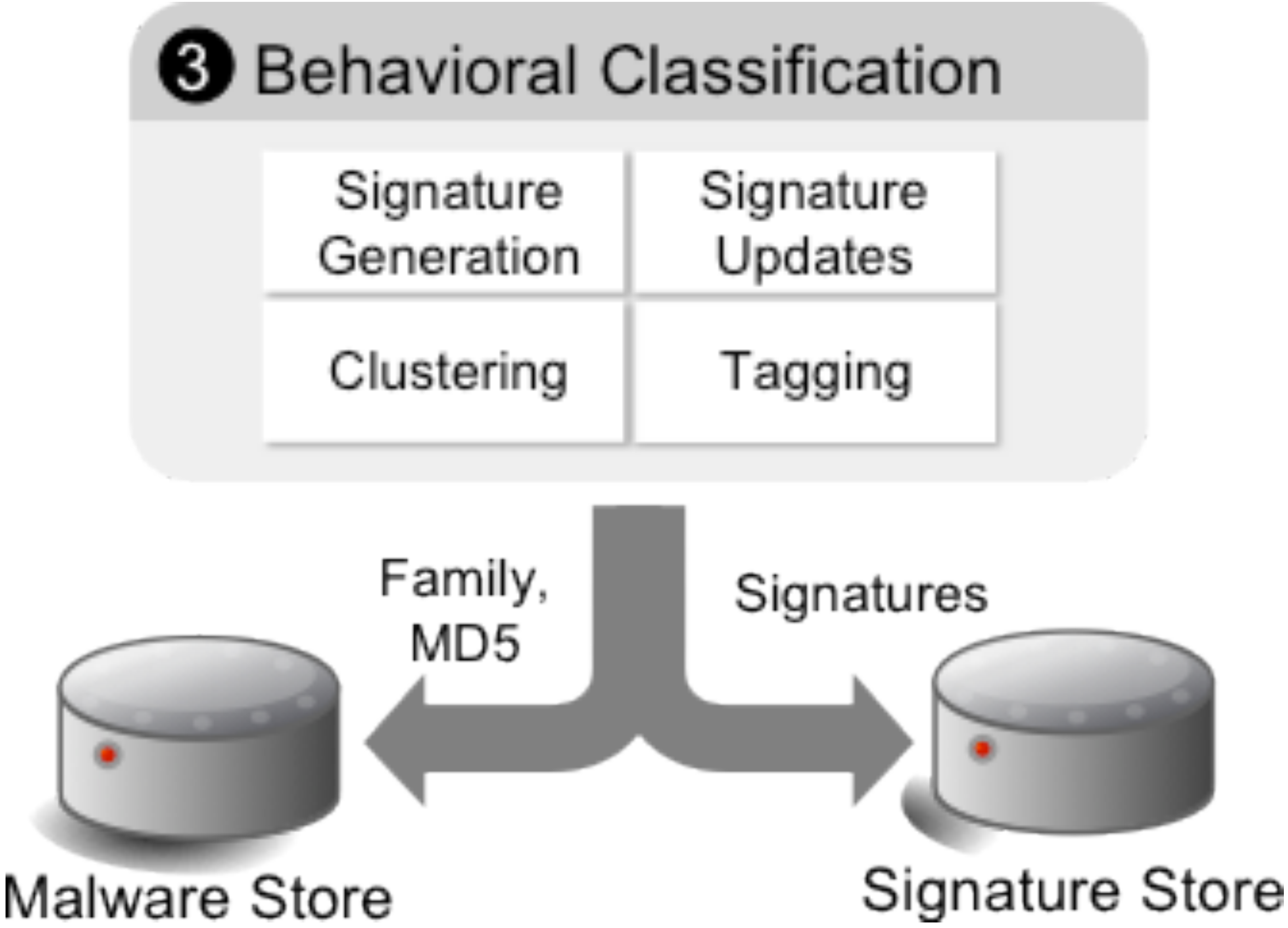


Running Malware

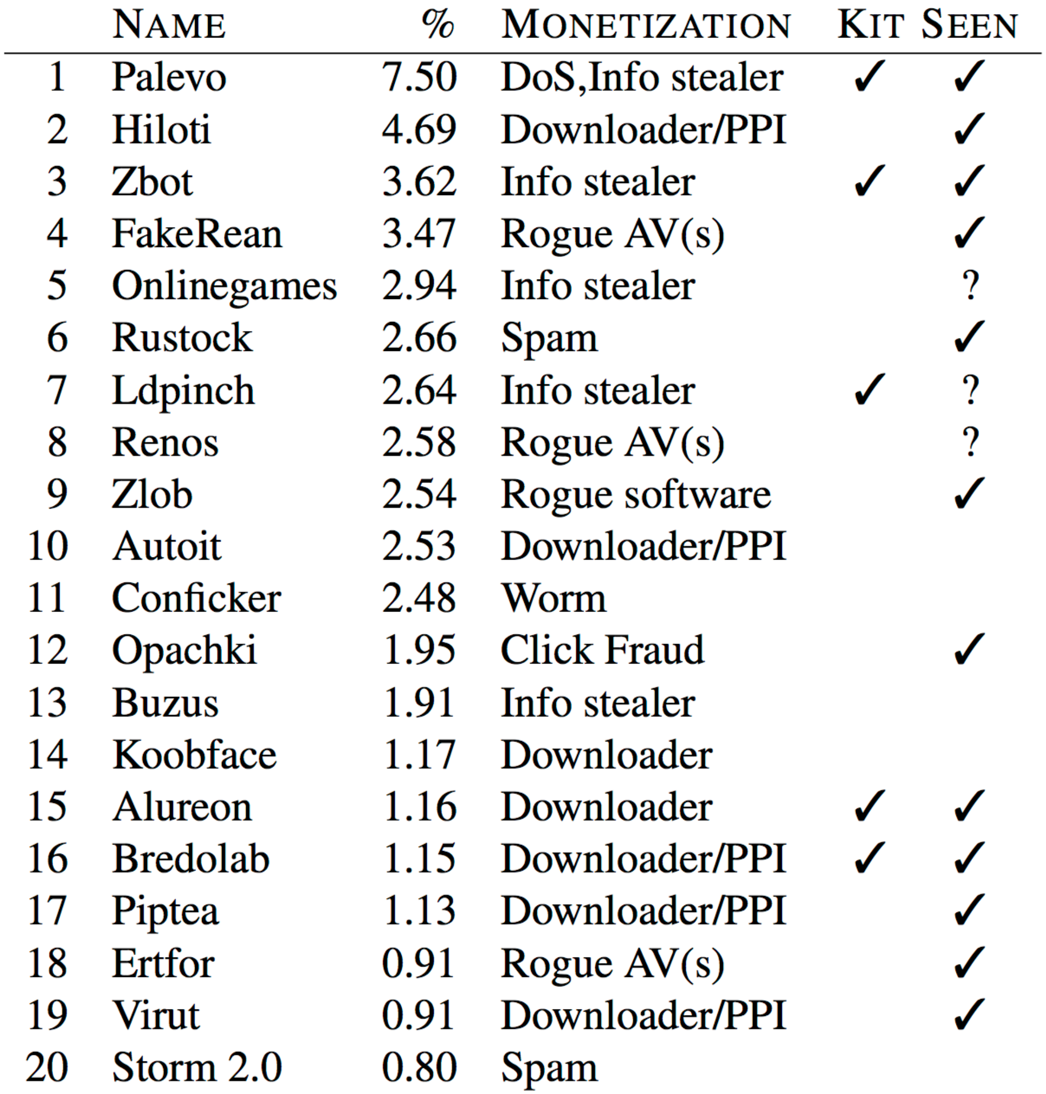


GQ: Practical Containment for Measuring Modern Malware Systems
C. Kreibich, N. Weaver, C. Kanich, W. Cui, V. Paxson. IMC 2011.

Classifying Malware



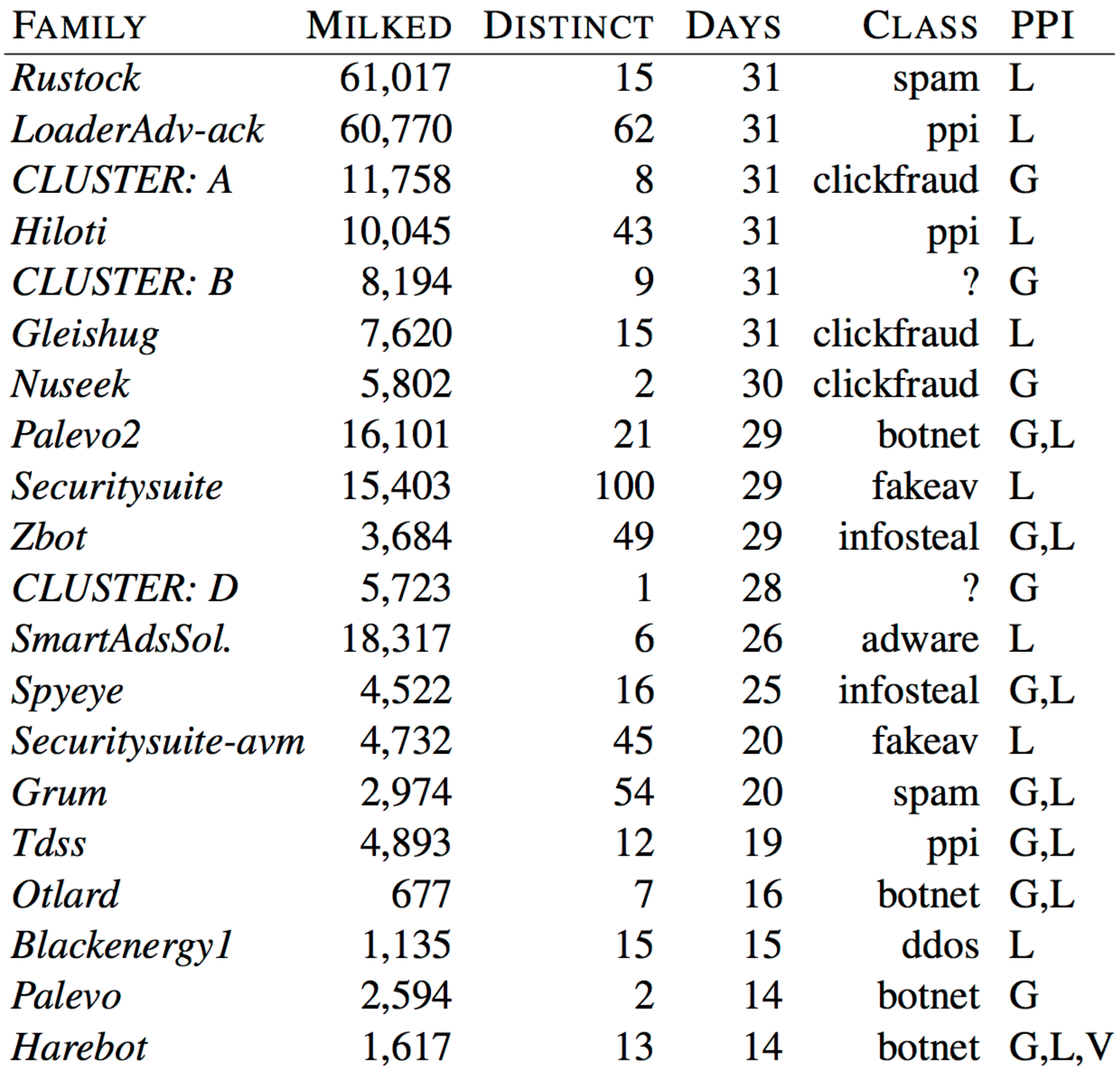
Malware Family Coverage



	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		

12 / 20 Being dropped by PPI!

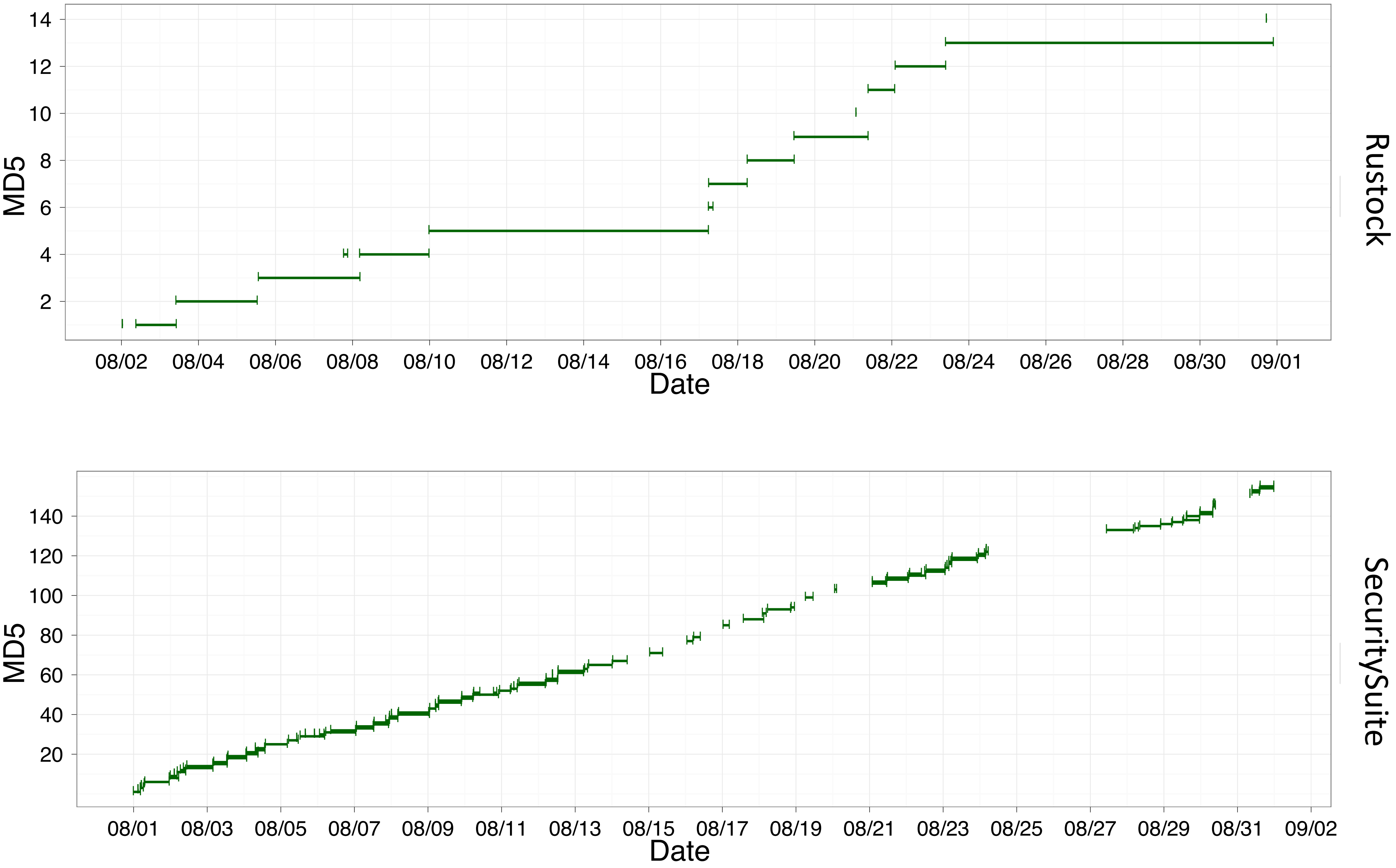
Most Seen Families: Aug 2010



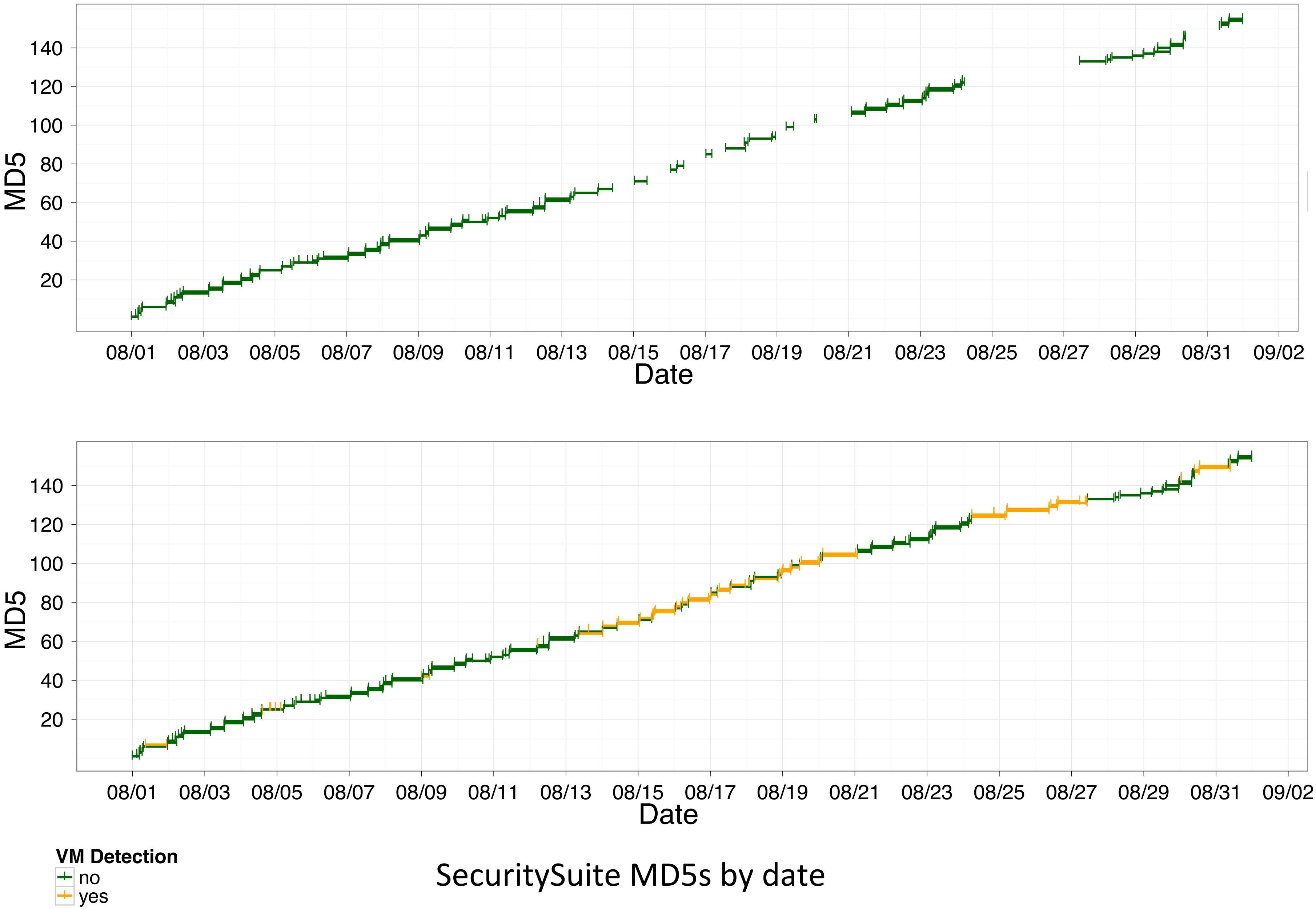
FAMILY	MILKED	DISTINCT	DAYS	CLASS	PPI
Rustock	61,017	15	31	spam	L
LoaderAdv-ack	60,770	62	31	ppi	L
CLUSTER: A	11,758	8	31	clickfraud	G
Hiloti	10,045	43	31	ppi	L
CLUSTER: B	8,194	9	31	?	G
Gleishug	7,620	15	31	clickfraud	L
Nuseek	5,802	2	30	clickfraud	G
Palevo2	16,101	21	29	botnet	G,L
Securitysuite	15,403	100	29	fakeav	L
Zbot	3,684	49	29	infosteal	G,L
CLUSTER: D	5,723	1	28	?	G
SmartAdsSol.	18,317	6	26	adware	L
Spyeye	4,522	16	25	infosteal	G,L
Securitysuite-avm	4,732	45	20	fakeav	L
Grum	2,974	54	20	spam	G,L
Tdss	4,893	12	19	ppi	G,L
Otlard	677	7	16	botnet	G,L
Blackenergy1	1,135	15	15	ddos	L
Palevo	2,594	2	14	botnet	G
Harebot	1,617	13	14	botnet	G,L,V

Binary Repacking

- Repacking or crypting
  - Changes program content without changing functionality
  - Frequency reflects concern about AV signatures
- PPI client binaries
  - Depends on family of malware
  - Average repacking every 11 days
- PPI affiliate binaries
  - Repacking done by PPI, usually daily
  - Zlob repacking done on-the-fly



MD5s by date for August, 2010 for two families of malware.

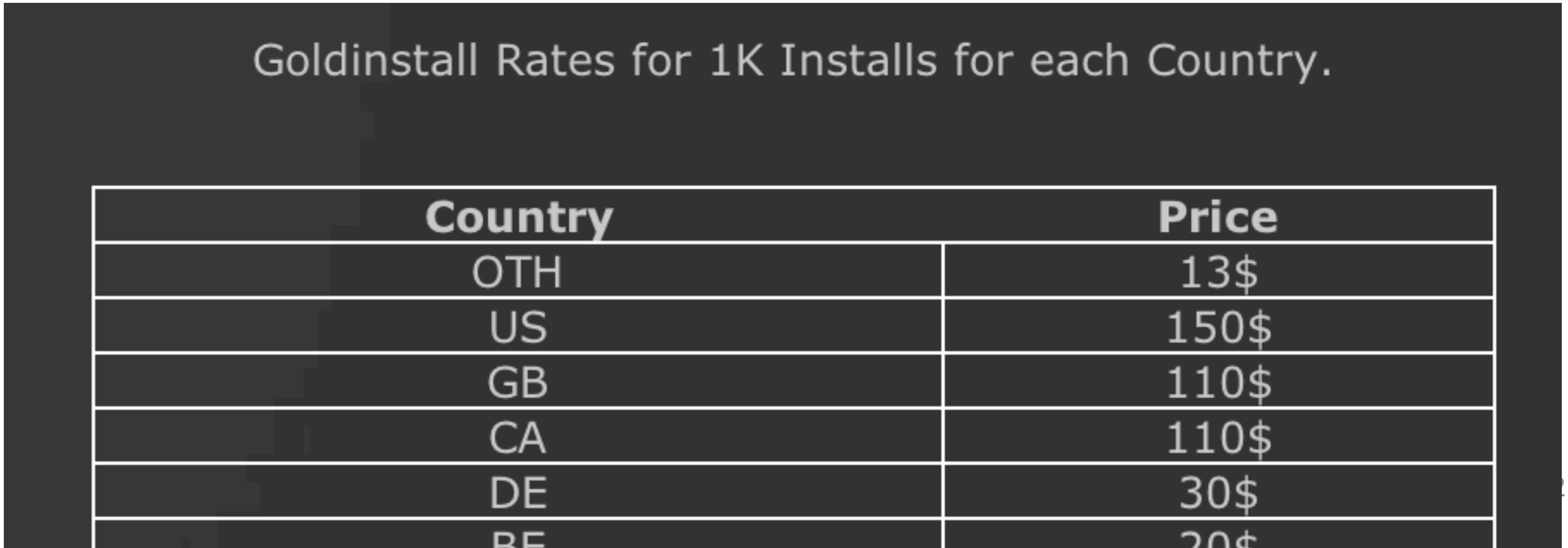


SecuritySuite MD5s by date

Geographic Distribution of Malware

- Use Tor exit points in 15 different countries
  - Verify exit-node IP using MaxMind GeoIP database
  - Zlob blocks Tor

- PPI clients are given a *choice* for installs



Goldinstall Rates for 1K Installs for each Country.

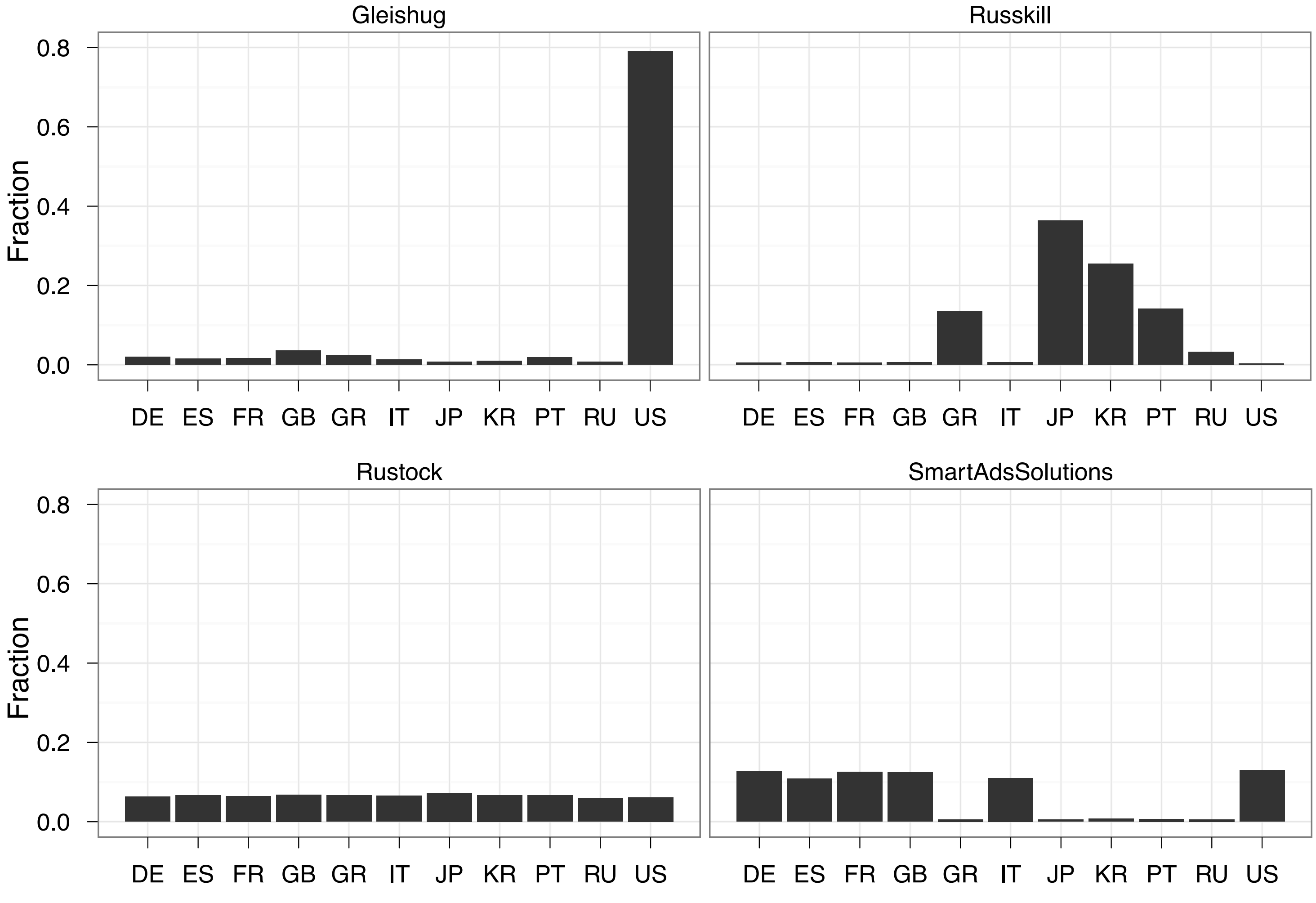
Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$

Geographic Distribution of Malware

- Use Tor exit points in 15 different countries
  - Verify exit-node IP using MaxMind GeoIP database
  - Zlob blocks Tor

- PPI clients are given a *choice* for installs
  - Prices vary depending on install location
  - Clients monetize hosts differently
    - Localization of Fake AV
    - Stolen credit card value varies
    - Legal limitations

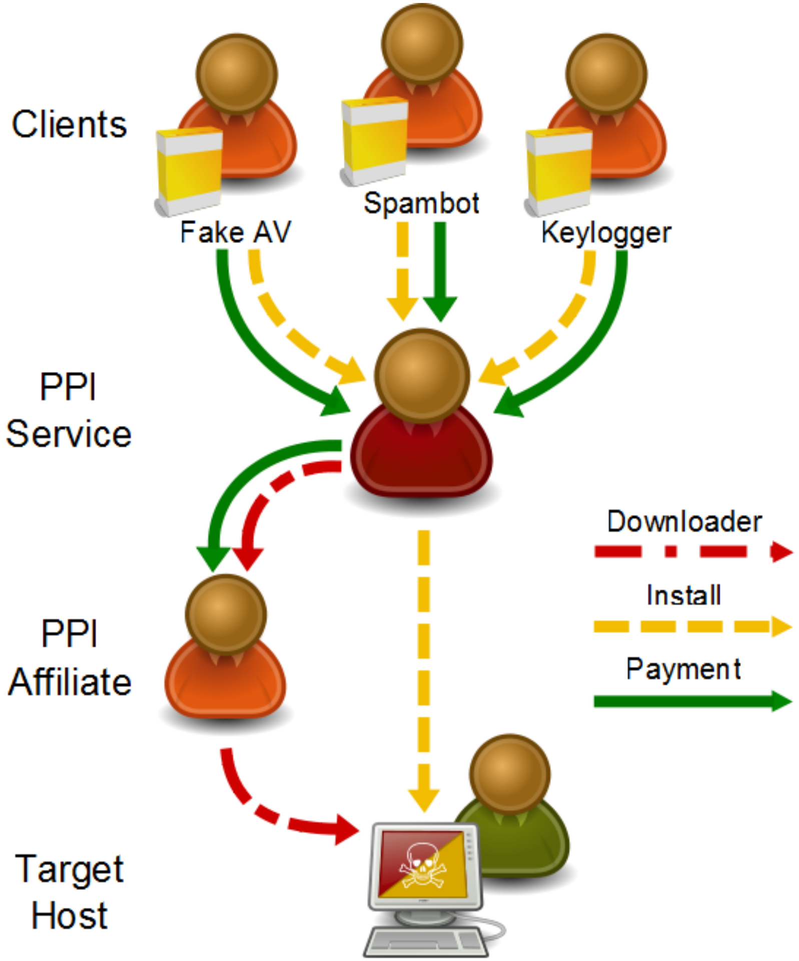
Distinct Geographic Distribution



Fraction of each binaries per family by Tor exit country

PPI Arbitrage

- Affiliate at one PPI, client at another!
- Exploit price differential
  - PPI 1: Buys 1k installs for $60 in Greece
  - PPI 2: Sells 1k installs for $40 in Greece



Conclusions

- First systematic study of the PPI ecosystem

- Infiltration provides *malware intelligence*
  - Used to perform several measurements

- Much of world's top malware using PPI
- Regular repacking of binaries
- Clients target geographic locations

Questions?