Global Phishing Survey

1H2012

Greg Aaron

Rod Rasmussen

APWG

Unifying the
Global Response
to Cybercrime

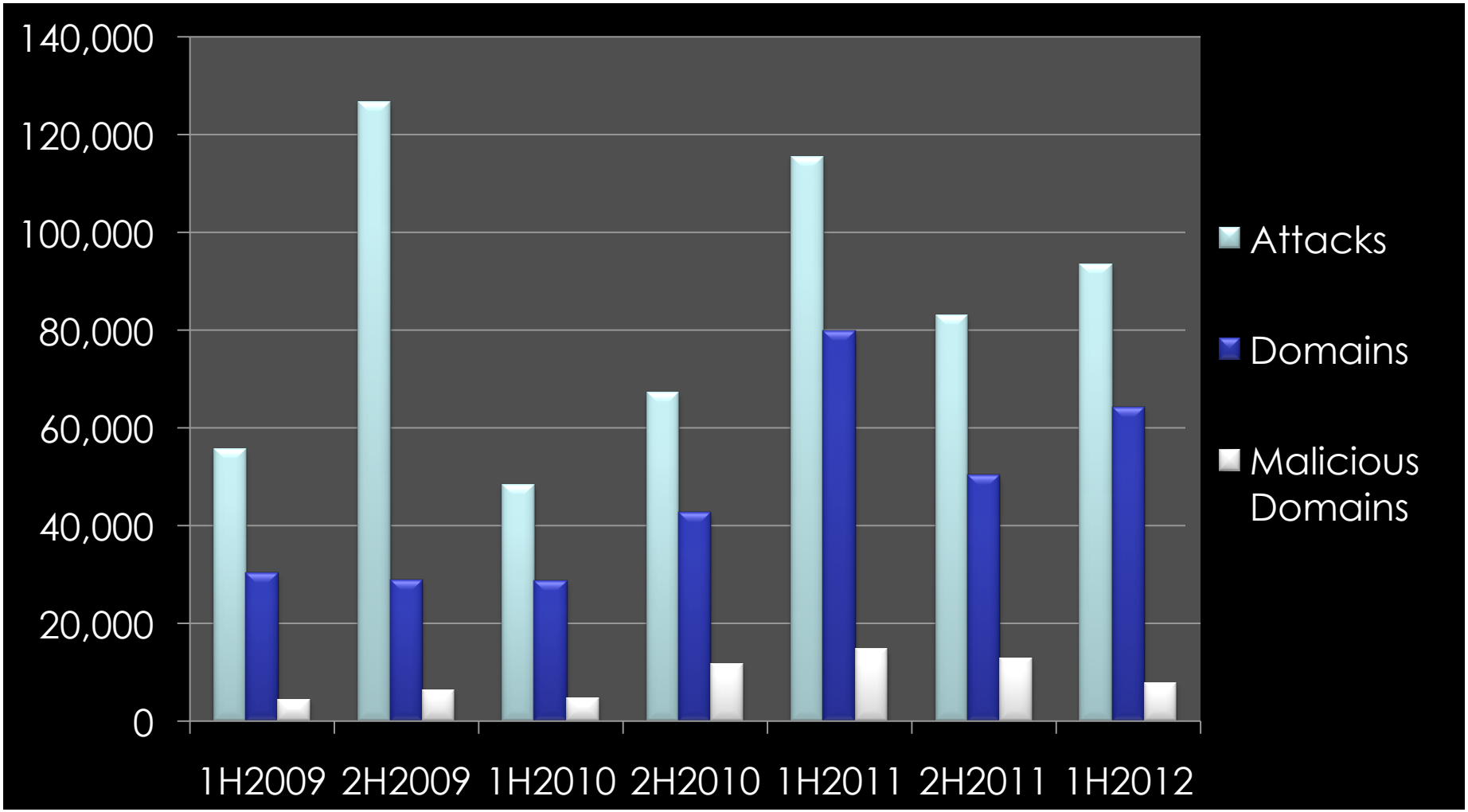
Goals

- Study domain names and URLs to:
- Provide a consistent benchmark for scope of phishing problems worldwide
- Understand what phishers are doing
- Identify new trends, hot-spots, success stories
- Suggest anti-abuse measures
- Collected data from APWG database, CNNIC, and several other sources

Data Sources

- Comprehensive sources:
  - APWG feed, phishing feeds, private sources, honeypots, CNNIC / APAC, DomainTools
- Millions of phishing URLs → small number of domain names and attacks.
- 240 million domain names in the world's registries

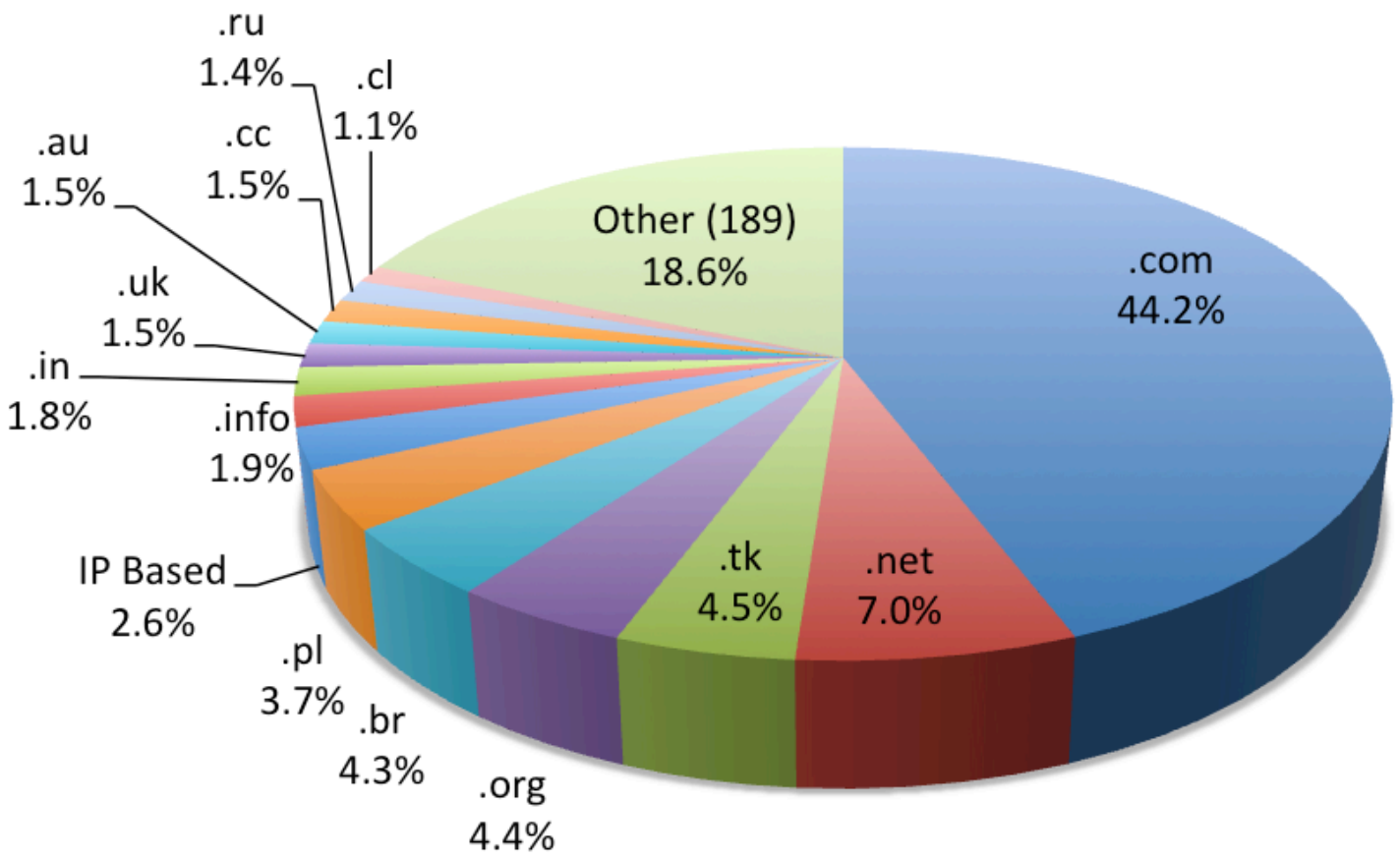
Overview


140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
1H2009
2H2009
1H2010
2H2010
1H2011
2H2011
1H2012
Attacks
Domains
Malicious Domains

Basic Statistics

	1H2012	2H2011	1H2011	2H2010	1H2010
Phishing domain names	64,204	50,298	79,753	42,624	28,646
Attacks	93,462	83,083	115,472	67,677	48,244
TLDs used	202	190	200	183	177
IP-based phish (unique IPs)	1,864	1,720	2,385	2,318	2,018
Maliciously registered domains	7,712	12,895	14,650	11,769	4,755
IDN domains	58	36	33	10	10
Targets	486	487	520	587	568

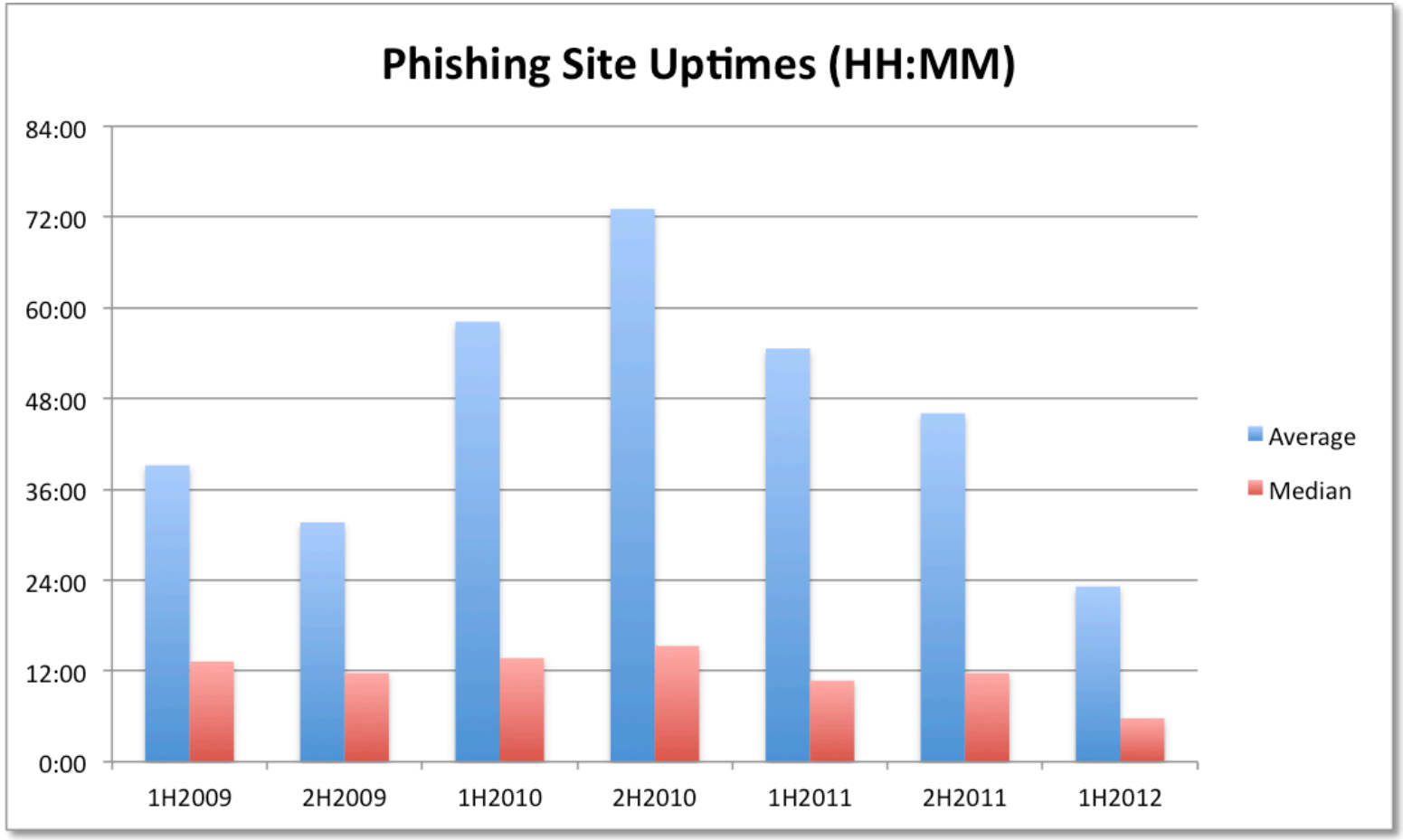
All Phishing Attacks by TLD, 1H2012

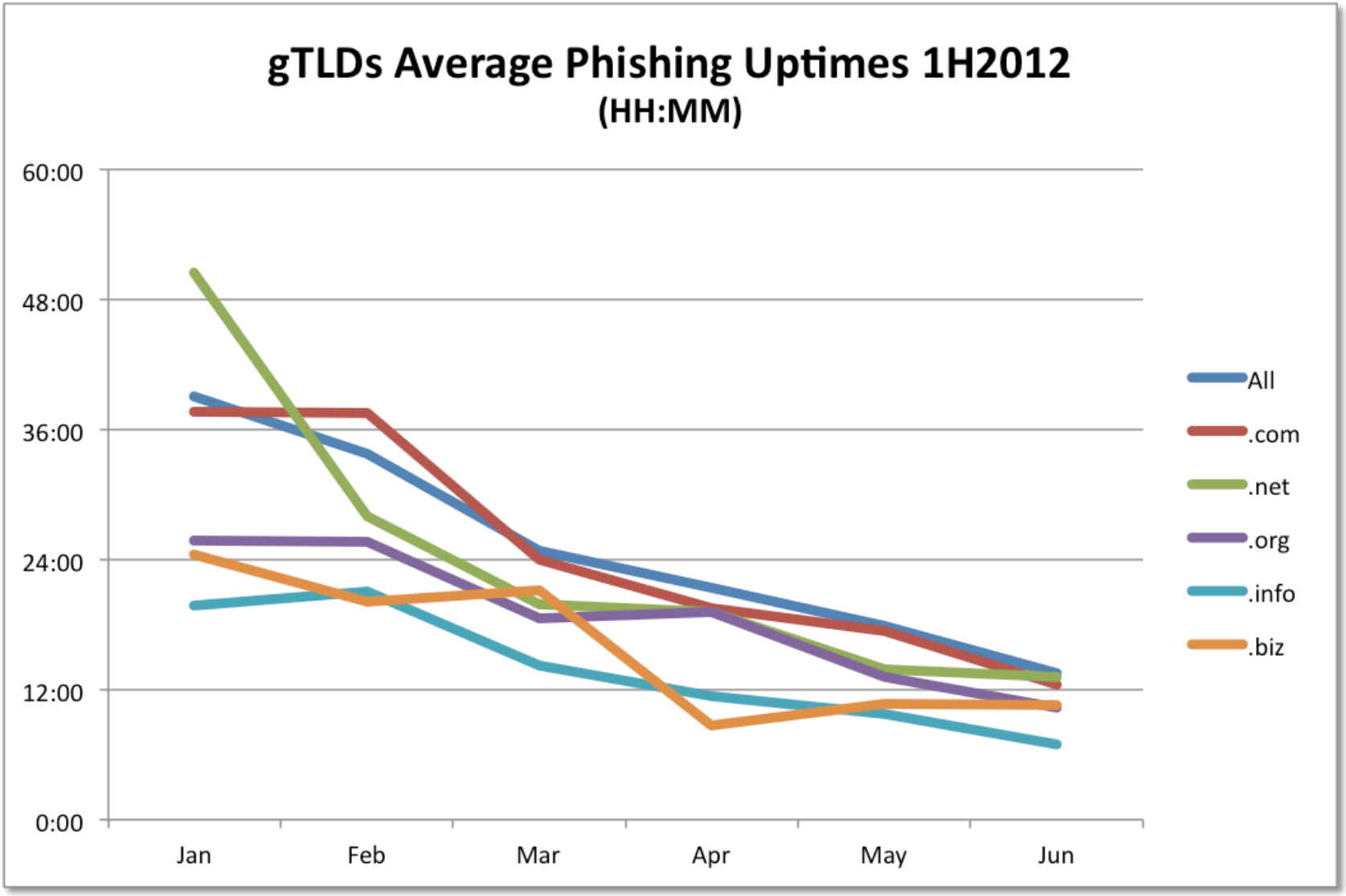


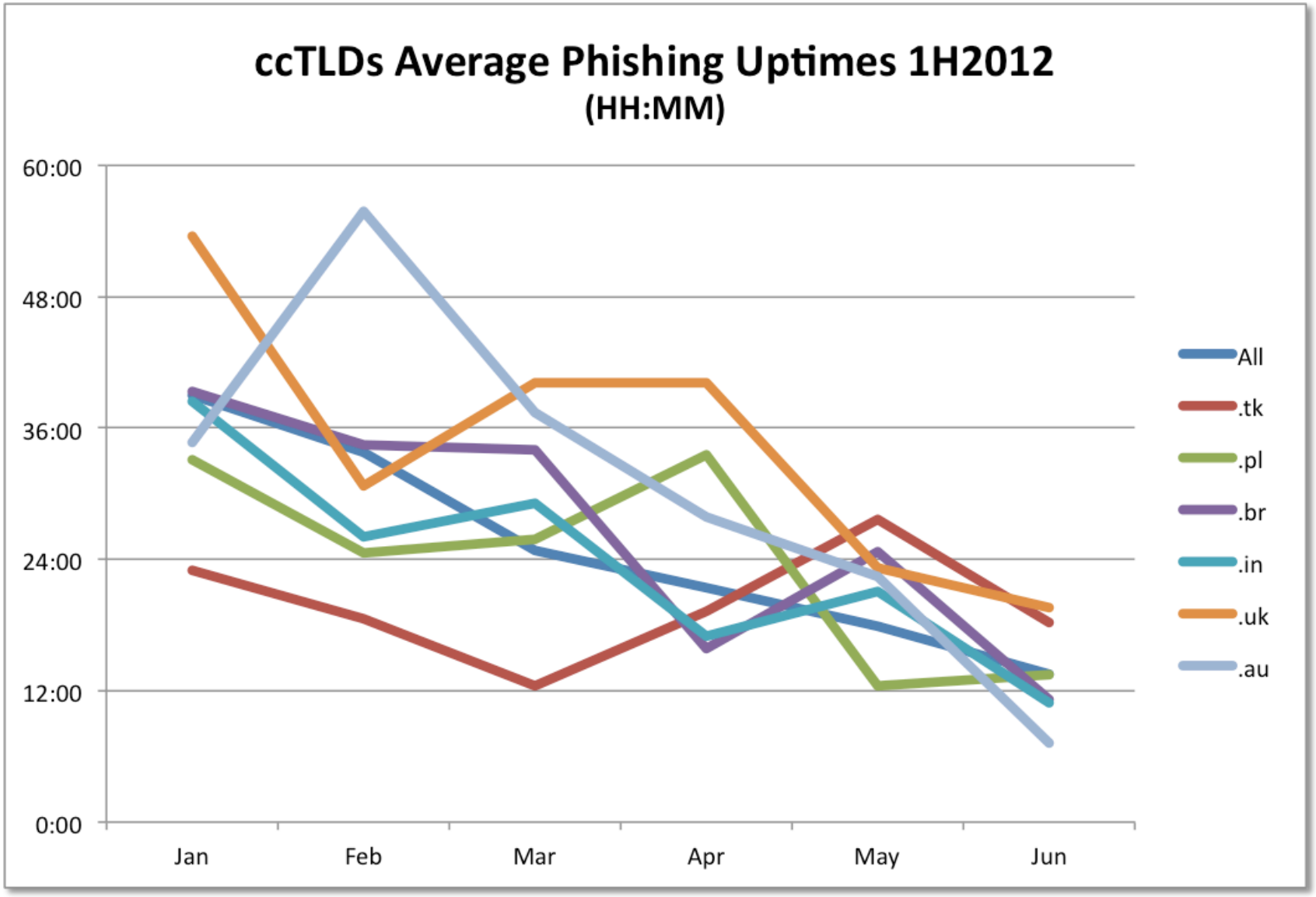
Phishing by TLD: Score

Rank	TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used 1H2012	Domains in registry, May 2012	Score: Phish per 10,000 domains 1H2012
1	cl	Chile	1,024	831	383,100	21.7
2	pe	Peru	126	115	61,530	18.7
3	id	Indonesia	113	95	78,000	12.2
4	th	Thailand	122	77	69,490	11.1
5	br	Brazil	4,039	3,207	2,959,495	10.8
6	ec	Ecuador	36	31	30,001	10.3
7	ro	Romania	967	533	576,323	9.2
8	za	South Africa	764	644	779,500	8.3
9	in	India	1,690	1,351	1,674,552	8.1
10	uy	Uruguay	35	29	36,908	7.9

Phishing Site Uptimes 1H2012:
23:10 hours average, 5:45 median

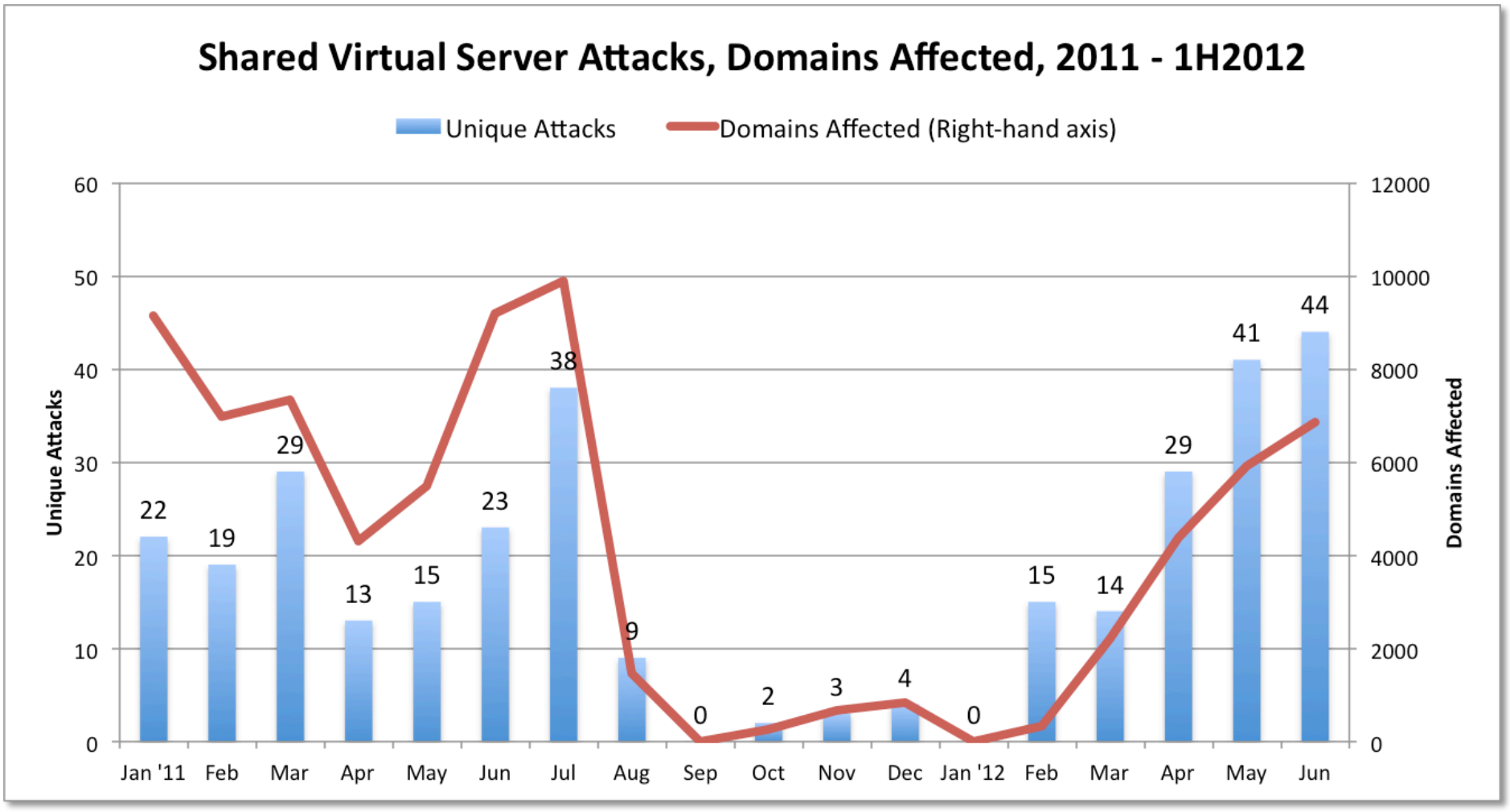



gTLDs Average Phishing Uptimes 1H2012
(HH:MM)
60:00
48:00
36:00
24:00
12:00
0:00
Jan
Feb
Mar
Apr
May
Jun
All
.com
.net
.org
.info
.biz


ccTLDs Average Phishing Uptimes 1H2012
(HH:MM)
60:00
48:00
36:00
24:00
12:00
0:00
Jan
Feb
Mar
Apr
May
Jun
All
.tk
.pl
.br
.in
.uk
.au

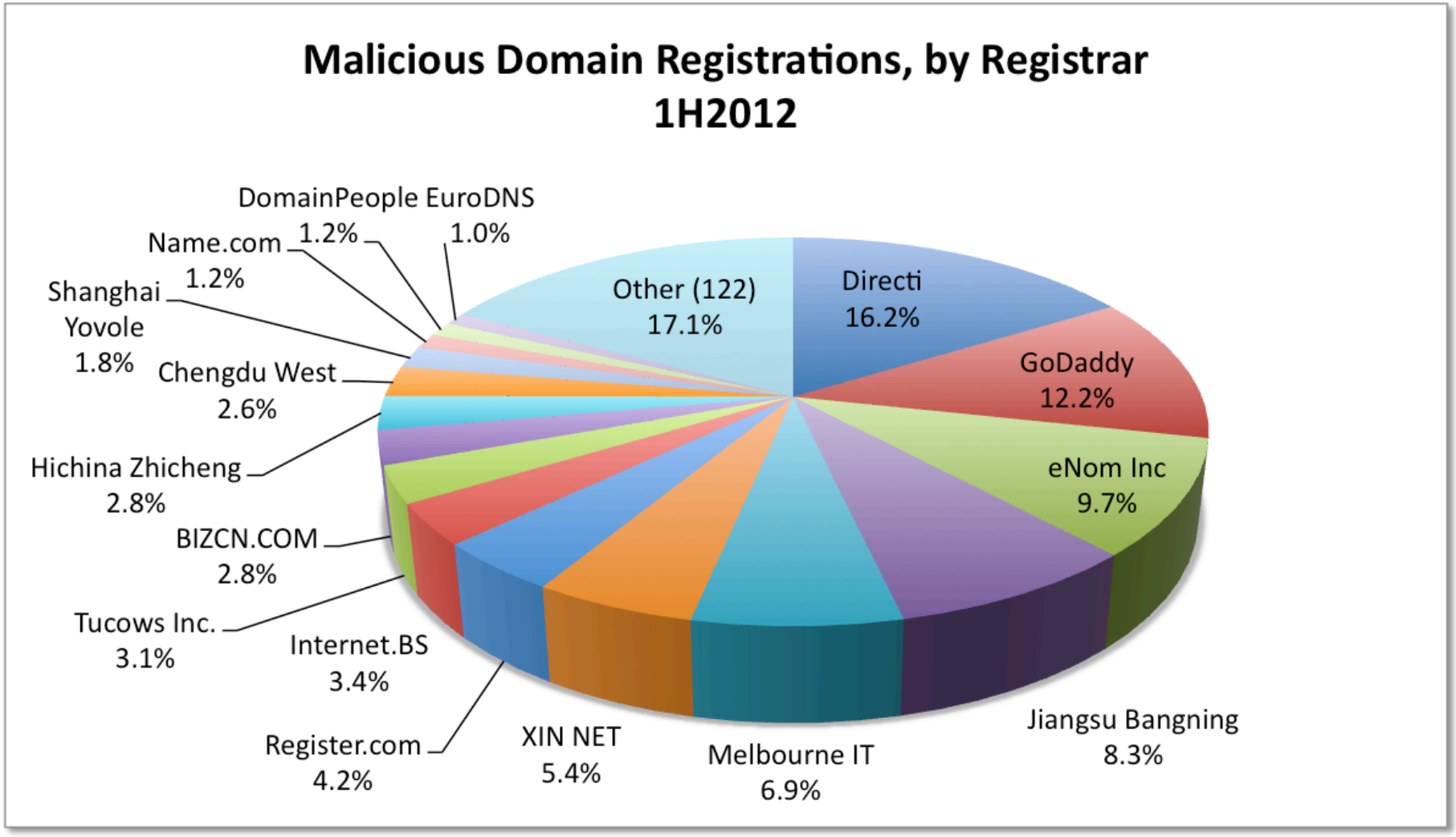
Virtual Server Hacking

- Phisher compromises server with single phishing site
- Updates server configuration to serve same site on ALL domains
- Great for spamming.
- 143 mass incidents, each involving at least 50 domains.
- **Involved 21,845 unique attacks, each using a different domain name. This was 23% of all phishing attacks worldwide.**

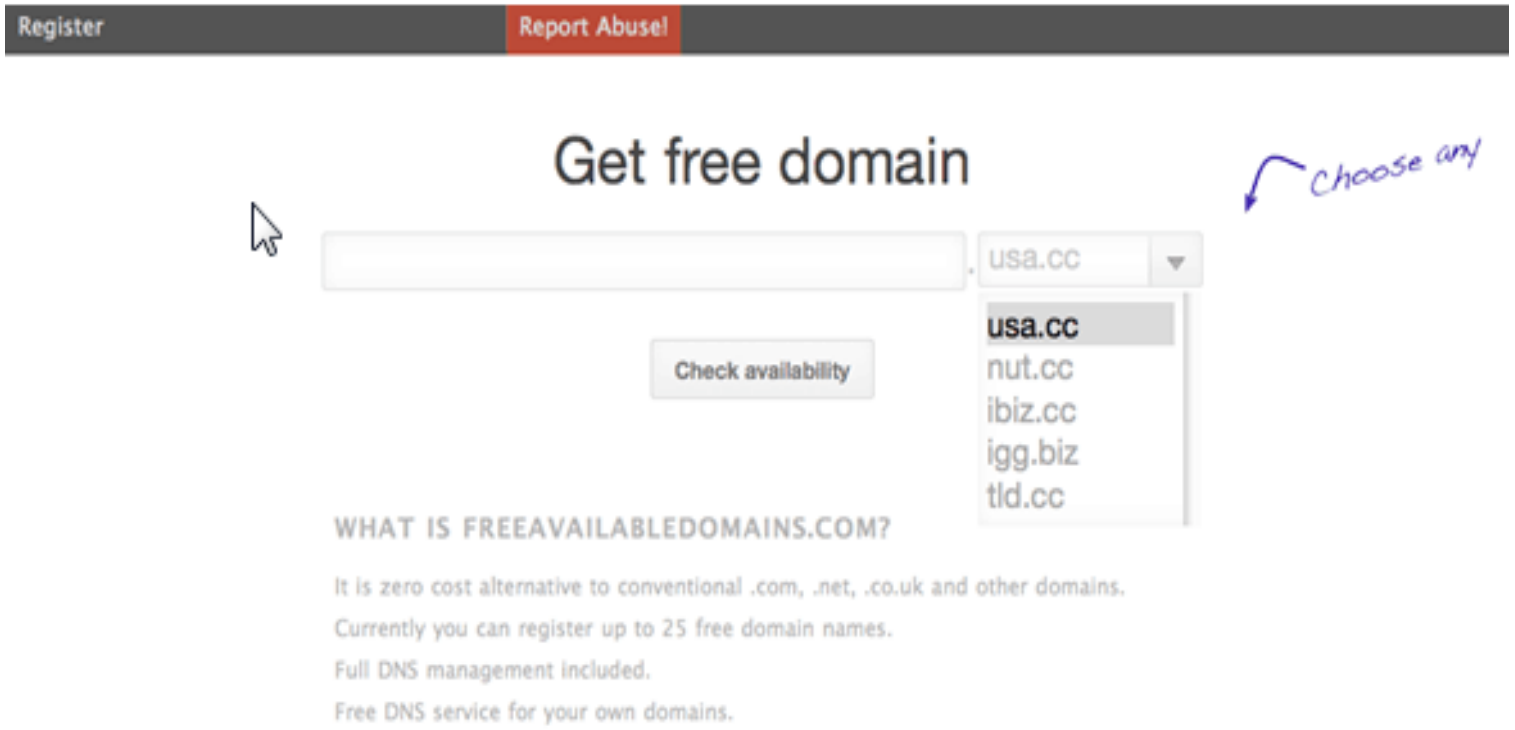


Phishing by Registrar

Rank	Registrar	Malicious Domain Names used for phishing 1H2012	TLD domains at registrar, September 2012	Score: Phish per 10,000 domains 1H2012
1	Shanghi Yovole Networks Inc.	63	1,537	44.2
2	Chengdu West Dimension Digital Technology Co.	88	3,177	30.9
3	Jiangsu Bangning Science and Technology Co. Ltd.	287	76,858	3.9
4	Internet.BS Corp.	118	89,402	1.5
5	BIZCN.COM, INC.	97	278,109	0.4
6	Directi Internet Solutions Pvt. Ltd. dba PublicDomainRegistry.com	558	1,724,071	0.4
7	Xin Net Technology Corp.	184	980,268	0.2

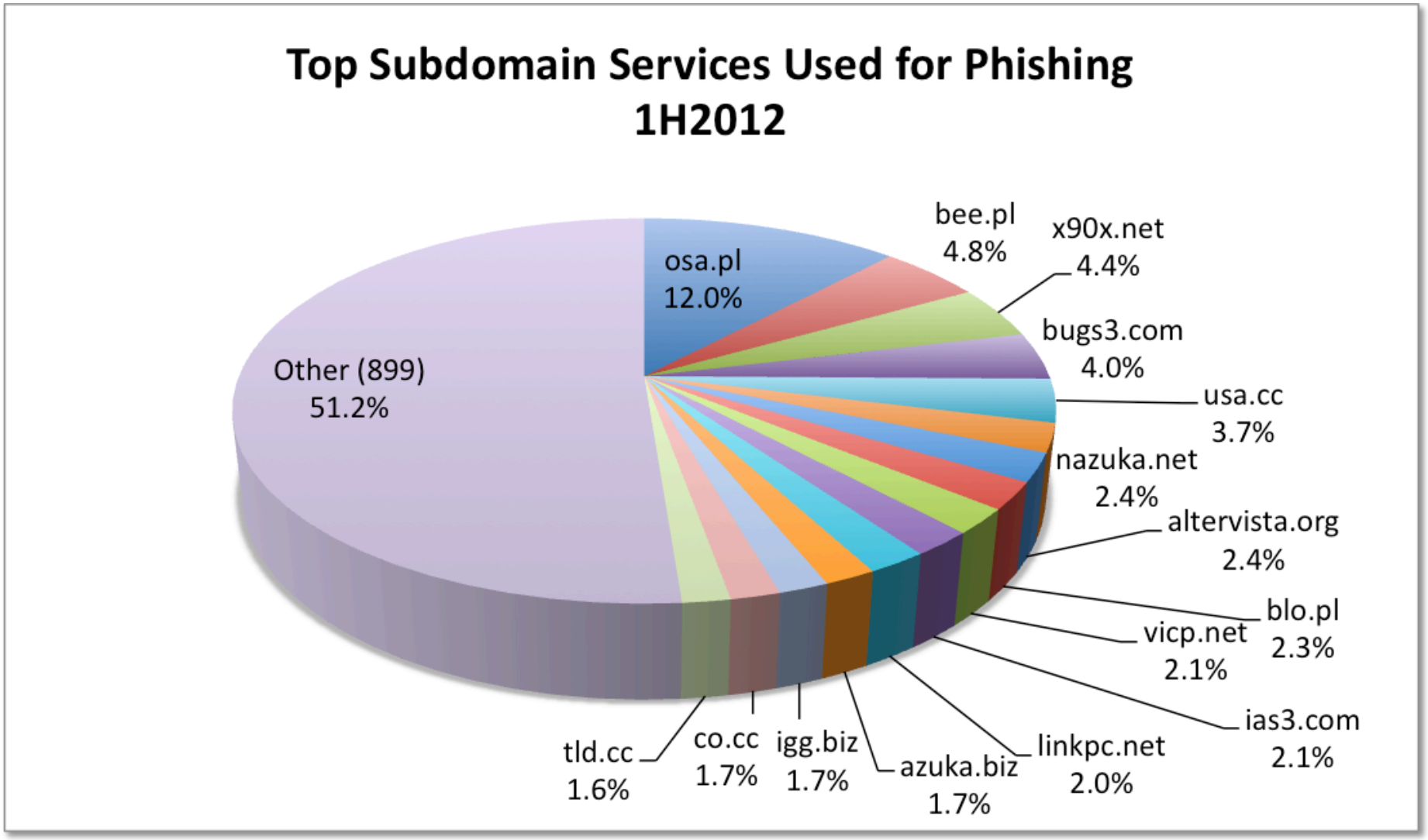

Malicious Domain Registrations, by Registrar
1H2012
DomainPeople 1.2%
EuroDNS 1.0%
Name.com 1.2%
Shanghai Yovole 1.8%
Chengdu West 2.6%
Hichina Zhicheng 2.8%
BIZCN.COM 2.8%
Tucows Inc. 3.1%
Internet.BS 3.4%
Register.com 4.2%
XIN NET 5.4%
Melbourne IT 6.9%
Jiangsu Bangning 8.3%
eNom Inc 9.7%
GoDaddy 12.2%
Directi 16.2%
Other (122) 17.1%

Use of Subdomain Services



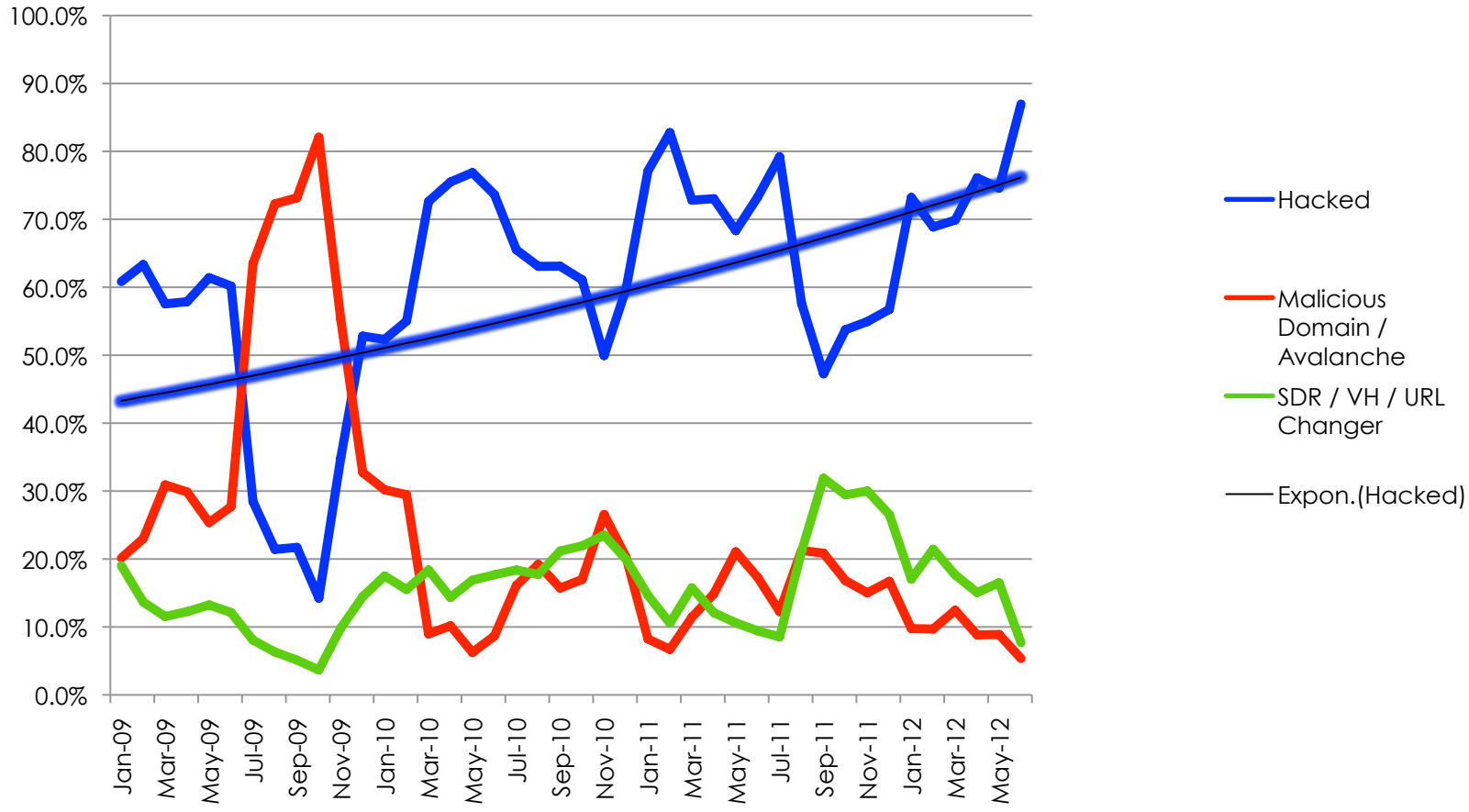
Subdomain Resellers

Provider	Rank	Attacks
bee.pl (osa.pl)	1	2,290
freeavailabledomains.com	2	958
x90x.net	3	799
Oray	4	548
ServersFree.com	5	541
nazuka.net	6	326
altervista.org	7	324
blo.pl	8	310
ias3.com	9	284
linkpc.net	10	275


Top Subdomain Services Used for Phishing
1H2012
osa.pl
12.0%
bee.pl
4.8%
x90x.net
4.4%
bugs3.com
4.0%
usa.cc
3.7%
nazuka.net
2.4%
altervista.org
2.4%
blo.pl
2.3%
vicp.net
2.1%
ias3.com
2.1%
linkpc.net
2.0%
azuka.biz
1.7%
igg.biz
1.7%
co.cc
1.7%
tld.cc
1.6%
Other (899)
51.2%

International Domain Names (IDNs)

Shifting Tactics



Thank you!

Full report on the APWG.org Web site, under "Resources"

APWG

Unifying the
Global Response
to Cybercrime