APWG Global Phishing Survey 2H2010

Rod Rasmussen

Greg Aaron

June 21, 2011

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
- Find hot-spots and success stories
- Suggest anti-abuse measures

Data Set

- Comprehensive sources: APWG, phishing feeds, private sources, honeypots
- Millions of phishing URLs → small number of domain names and attacks.
- Total of 205,715,855 domain names in the TLDs we have stats for ~ 99.5% of domain names in the world.

Basic Statistics

	2H2010	1H2010	2H2009	1H2009	2H2008
Phishing domain names	42,624	28,646	28,775	30,131	30,454
Attacks	67,677	48,244	126,697	55,698	56,959
TLDs used	183	177	173	171	170
IP-based phish (unique IPs)	2,318	2,018	2,031	3,563	2,809
Maliciously registered domains	11,769	4,755	6,372	4,382	5,591
IDN domains	10	10	12	13	10

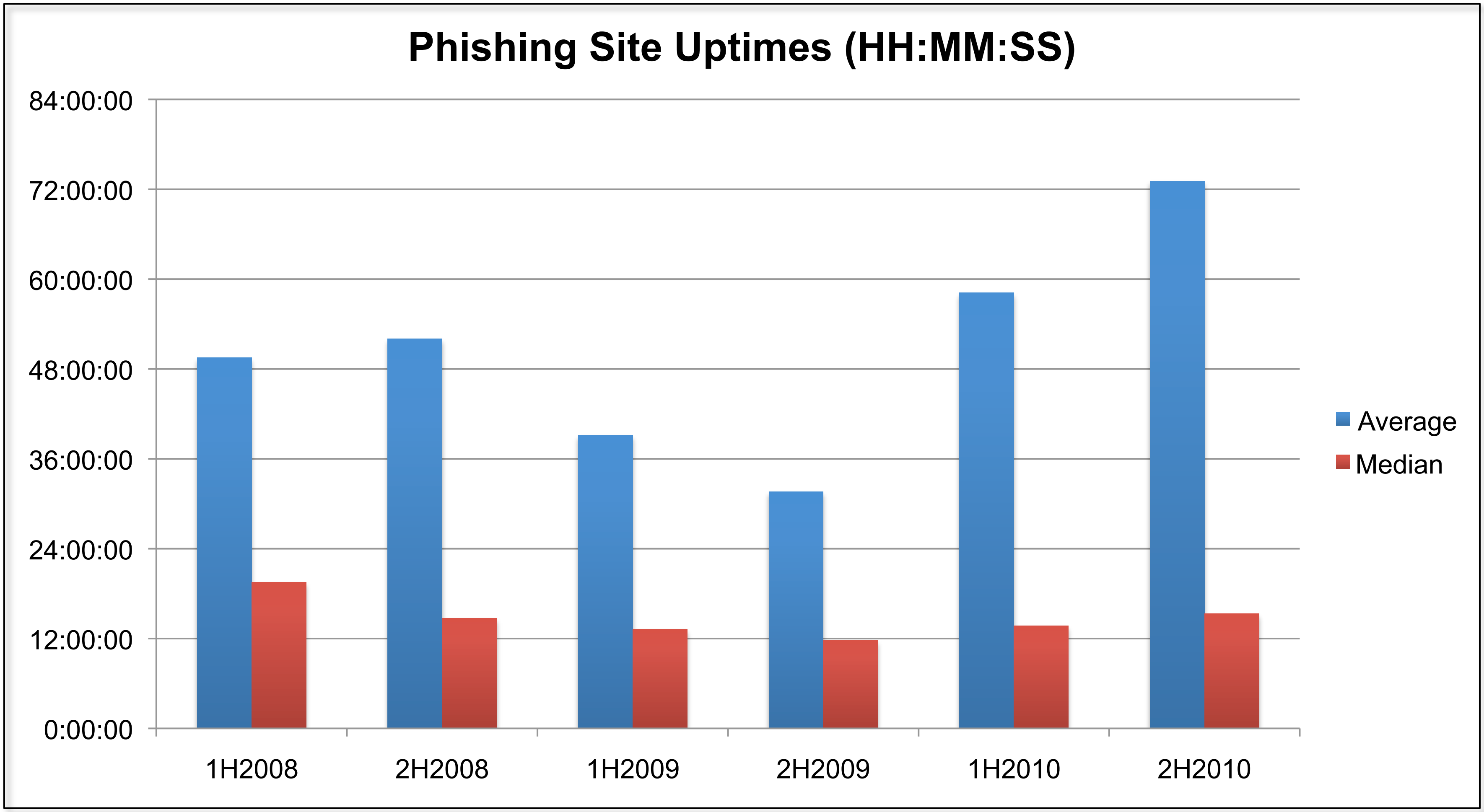
Phishing in China

- Data contribution from CNNIC and APAC (Anti-Phishing Alliance of China)
- Observers outside of China were detecting only about 20% of the phishing that targeted Chinese institutions.
- Attacks on Chinese banks, e-commerce sites.
  - Lures: Chinese-language e-mails, Chinese instant message services
  - WHOIS: registrants often listed in China, and list Chinese freemail services such as QQ.com

Phishing in China

- 2H2010: 12,282 attacks on Chinese institutions, using 6,382 unique domain names. (That’s 18% of all attacks worldwide)
- 74% of those attacks targeted Taobao.com
- Few .CN names used. CN registration policy became very restrictive in December 2009. Only 278 .CN names used in 2H2010, some hacked.
- Phishers simply switched to using other resources to phish Chinese targets:
  - Used 4,737 free CO.CC subdomains
  - Used large numbers of .COM, .TK, .INFO, .US, .IN domains
- Chinese phishers prefer to register domain names – only 8% looked hacked.

Phishing Site Uptime 2H2010:
73 hours average, 15:19 hours median

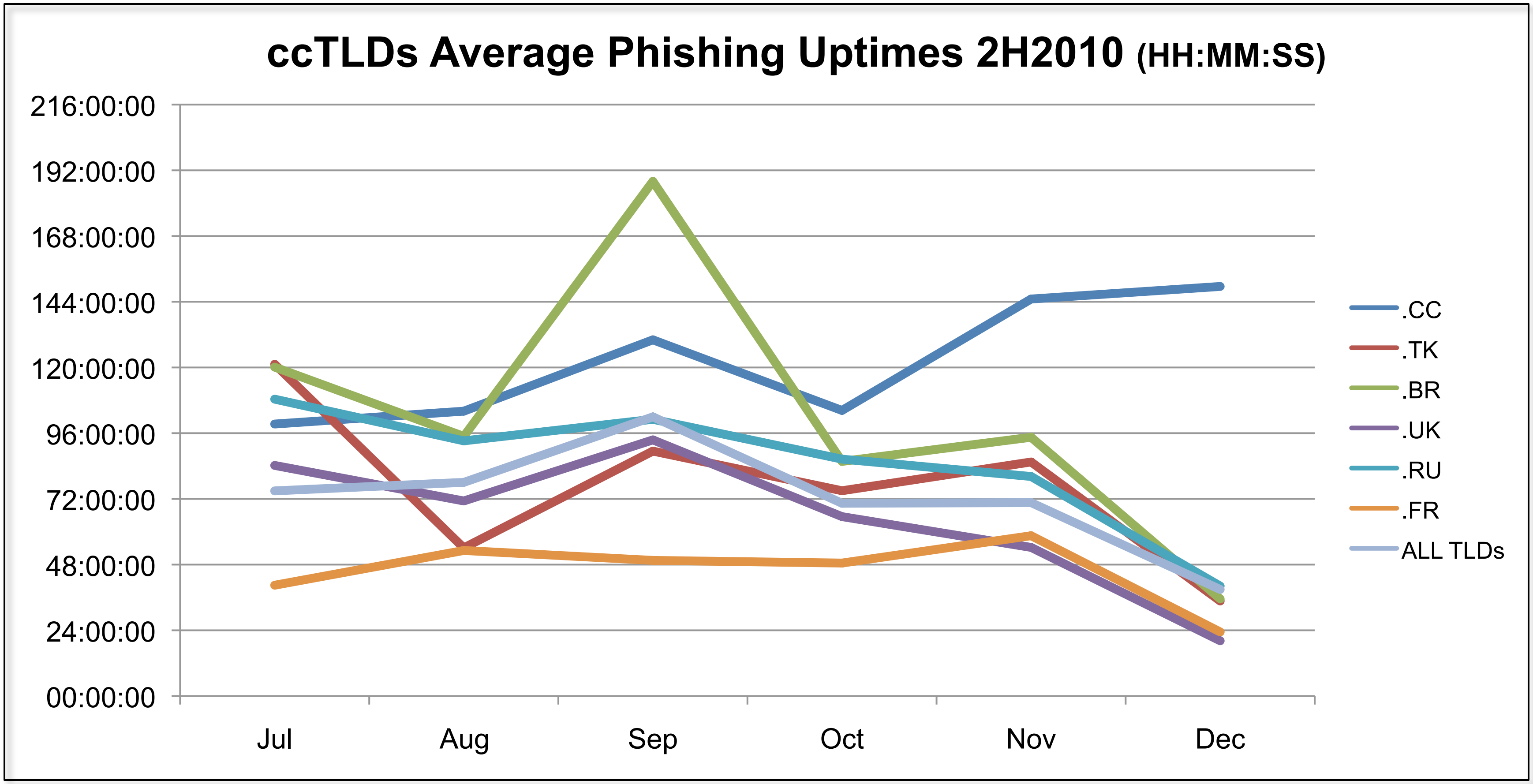


Why So High?

- Absence of Avalanche domains
- There were 4,963 phishing attacks using free CO.CC subdomains. Their median uptime was almost 60 hours – compared with 15:19 hours for all phish.
- Don’t know the uptimes for the phish uniquely recorded by CNNIC/APAC

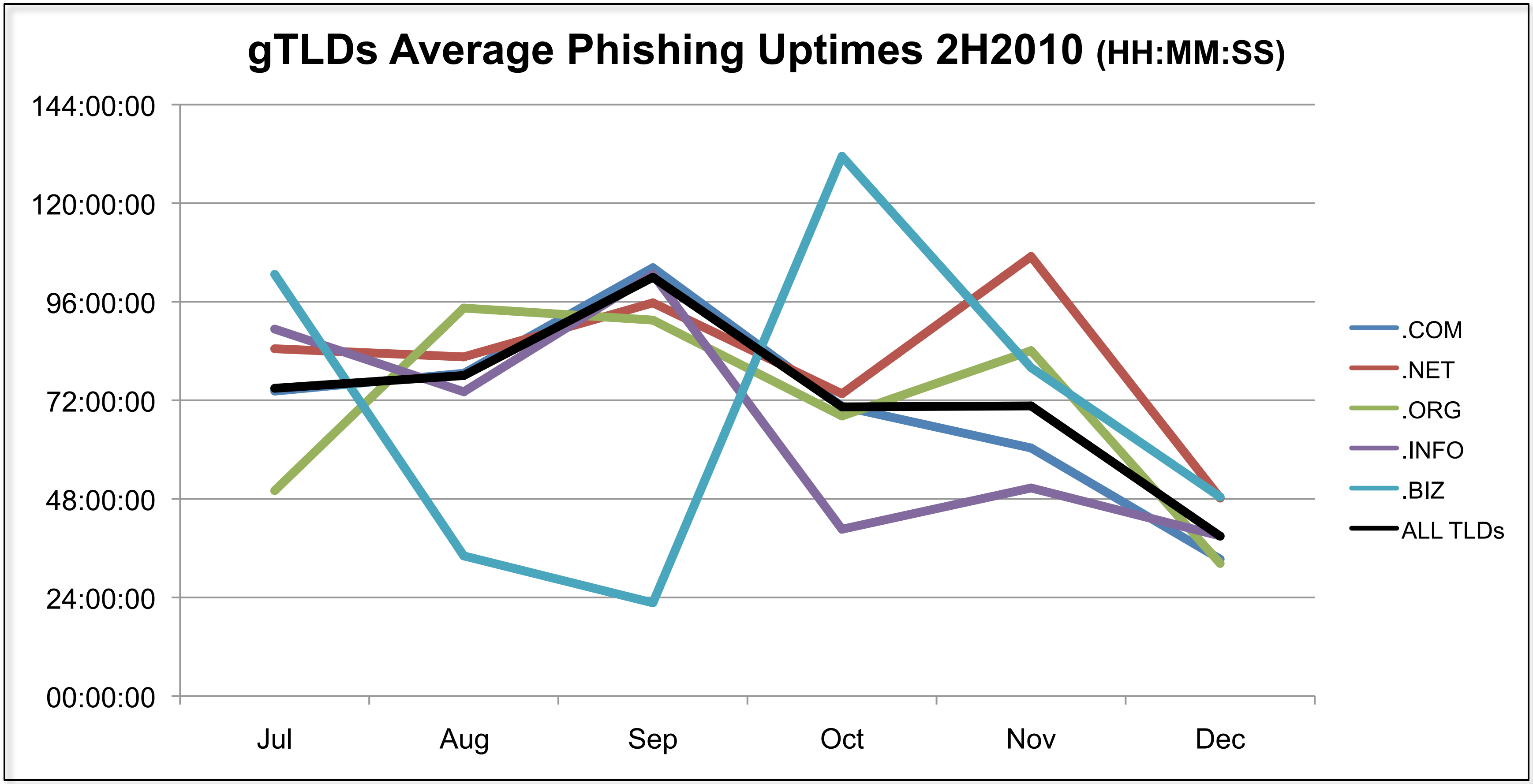
ccTLD Uptimes

(HH:MM:SS)

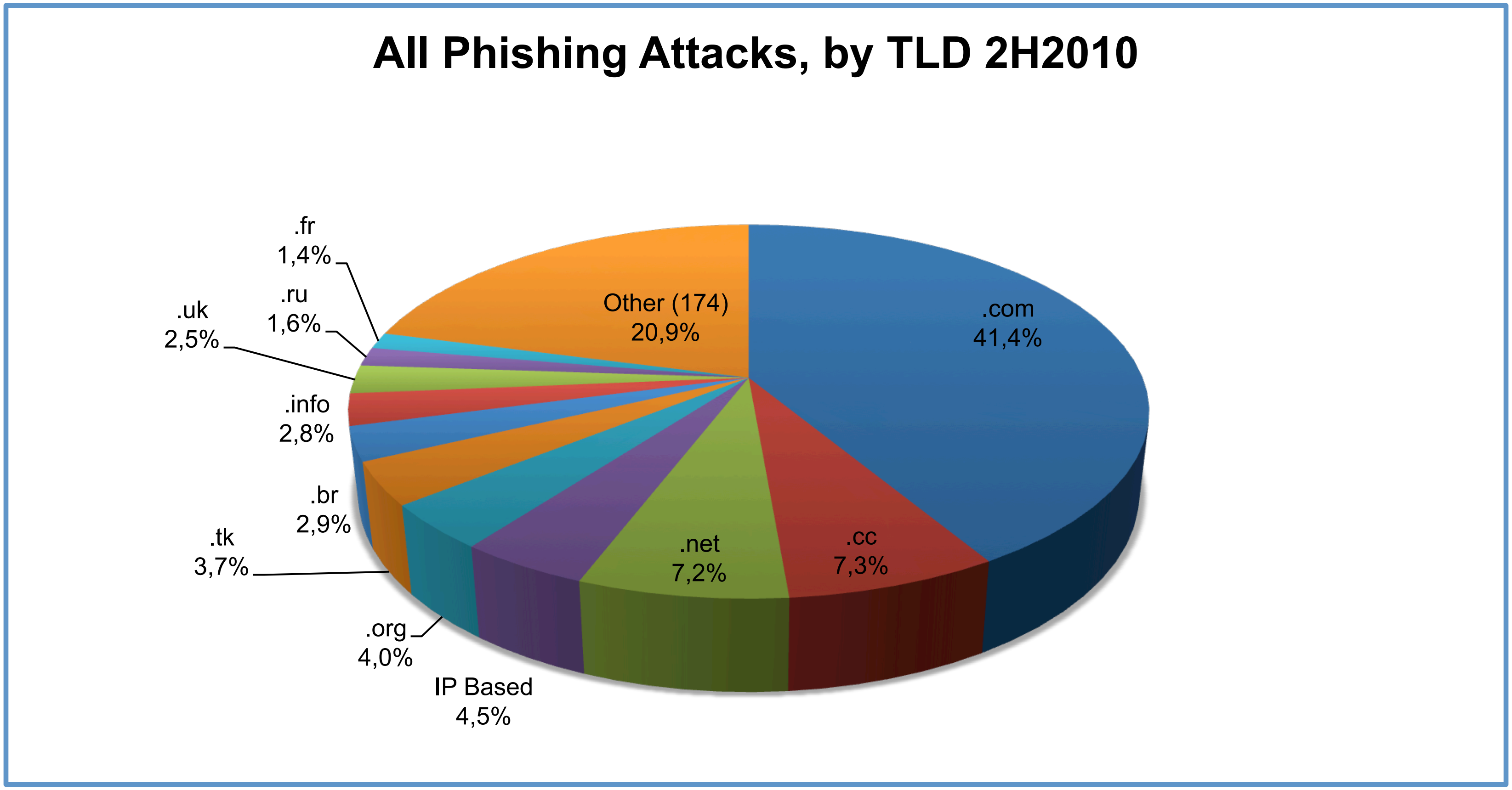


gTLD Uptimes

(HH:MM:SS)



Phishing Rates by TLD: roughly proportional by TLD size



Phishing by TLD: Score

- Metric: “Phishing Domains per 10,000”
  - Measures prevalence of phishing in a TLD
  - Median score: **3.2**
  - .COM score: **2.1**
  - Scores between 2.1 and 3.2 are “normal”
  - Scores skew higher for smaller TLDs.
- Metric: “Attacks per 10,000 Domains”

Top TLDs by Domain Score (minimum 30,000 domains and 25 phish)

RANK	TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010
1	.TH	Thailand	125	65	51,438	12.6	24.3
2	.IR	Iran	295	169	175,600	9.6	17.0
3	.MA	Morocco	73	34	36,669	9.3	20.2
4	.IE	Ireland	112	96	151,023	6.4	7.7
5	.TK	Tokelau	2,533	2,429	4,030,709	6.0	6.3
6 (tie)	.KZ	Kazakhstan	49	28	50,534	5.5	9.7
6 (tie)	.CC	Cocos (Keeling) Islands	4,963	55	100,000 (estimated)	5.5	496.3
8	.IN	India	523	421	791,165	5.3	6.6
9	.MY	Malaysia	68	55	108,211	5.1	6.5
10	.HU	Hungary	365	255	542,000	4.7	6.7

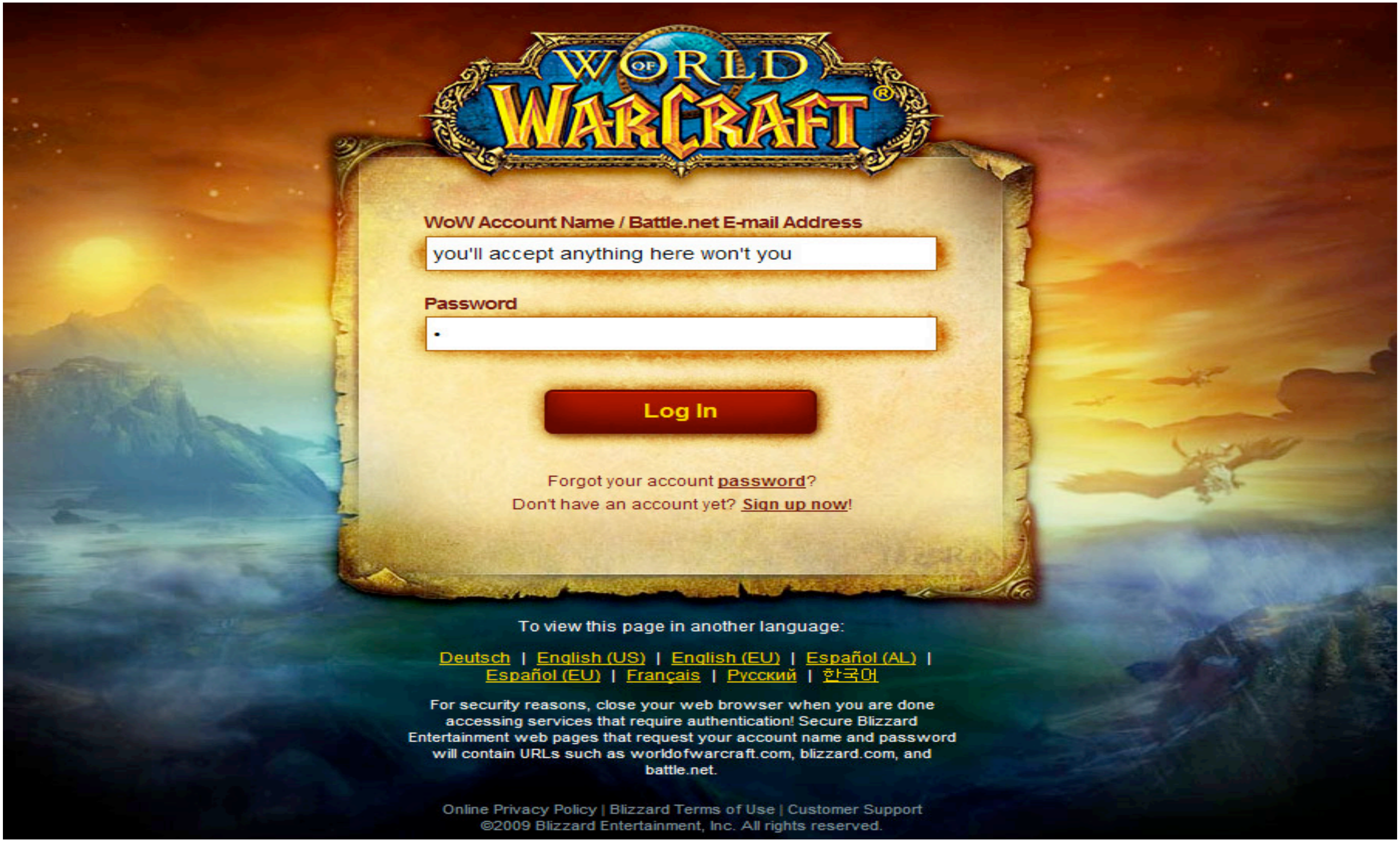
ICANN Singapore 41 19-24 June 2011

Malicious Domain Registrations

Of the 42,624 phishing domains:

- **~72% were compromised/hacked**
- **~28% were registered by phishers** (11,769). Most of those domains (6,382) were registered to attack Chinese targets.
- 9% of domains (1,503) contained a relevant brand name or brand misspelling. (Especially Taobao.com)

2,066 maliciously registered domains targeted WarCraft and Battle.net



WoW Account Name / Battle.net E-mail Address

you'll accept anything here won't you

Password

•

Forgot your account password?
Don't have an account yet? Sign up now!

To view this page in another language:

Deutsch | English (US) | English (EU) | Español (AL) | Español (EU) | Français | Русский | 한국어

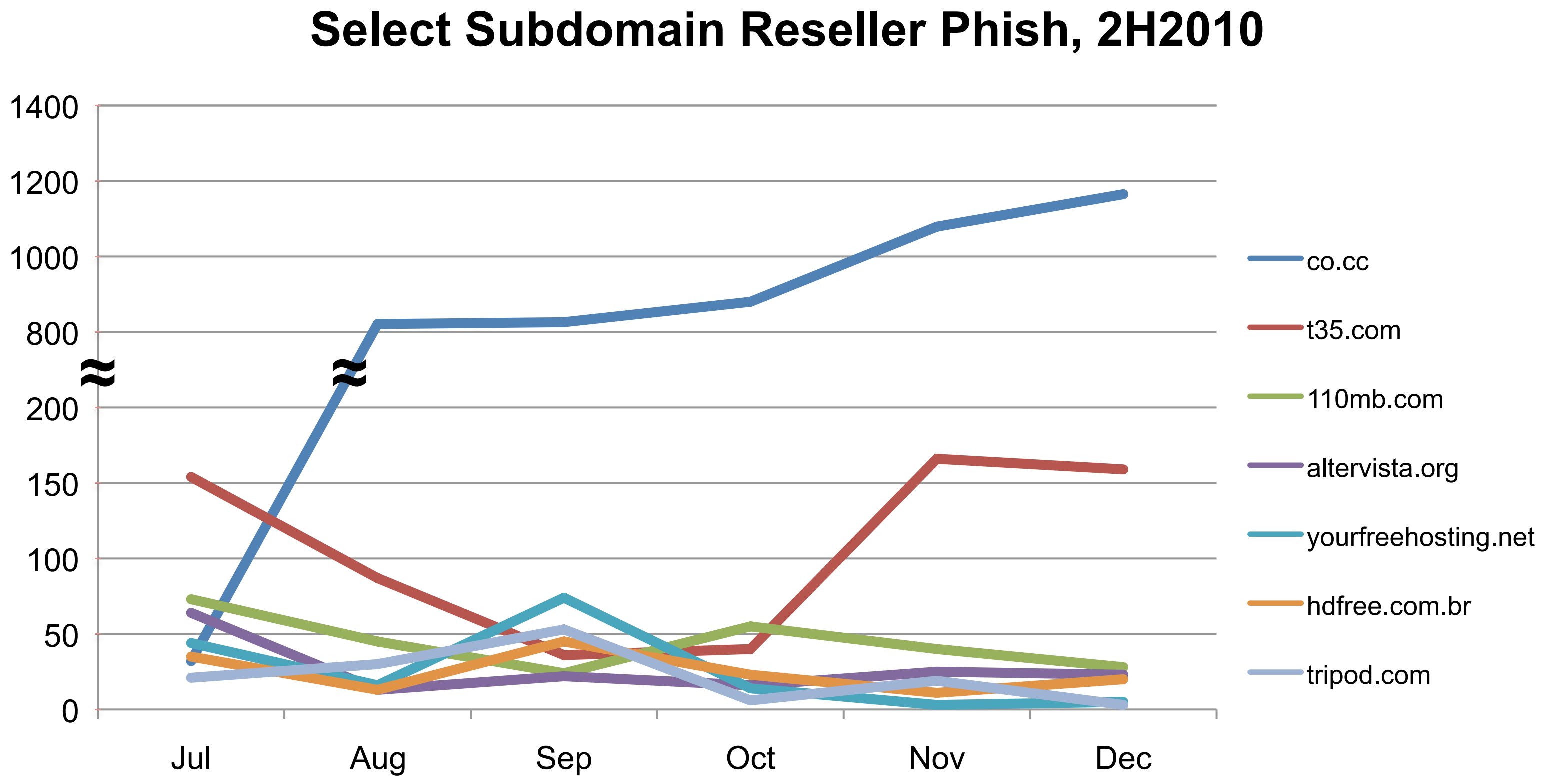
For security reasons, close your web browser when you are done accessing services that require authentication! Secure Blizzard Entertainment web pages that request your account name and password will contain URLs such as worldofwarcraft.com, blizzard.com, and battle.net.

Online Privacy Policy | Blizzard Terms of Use | Customer Support
©2009 Blizzard Entertainment, Inc. All rights reserved.

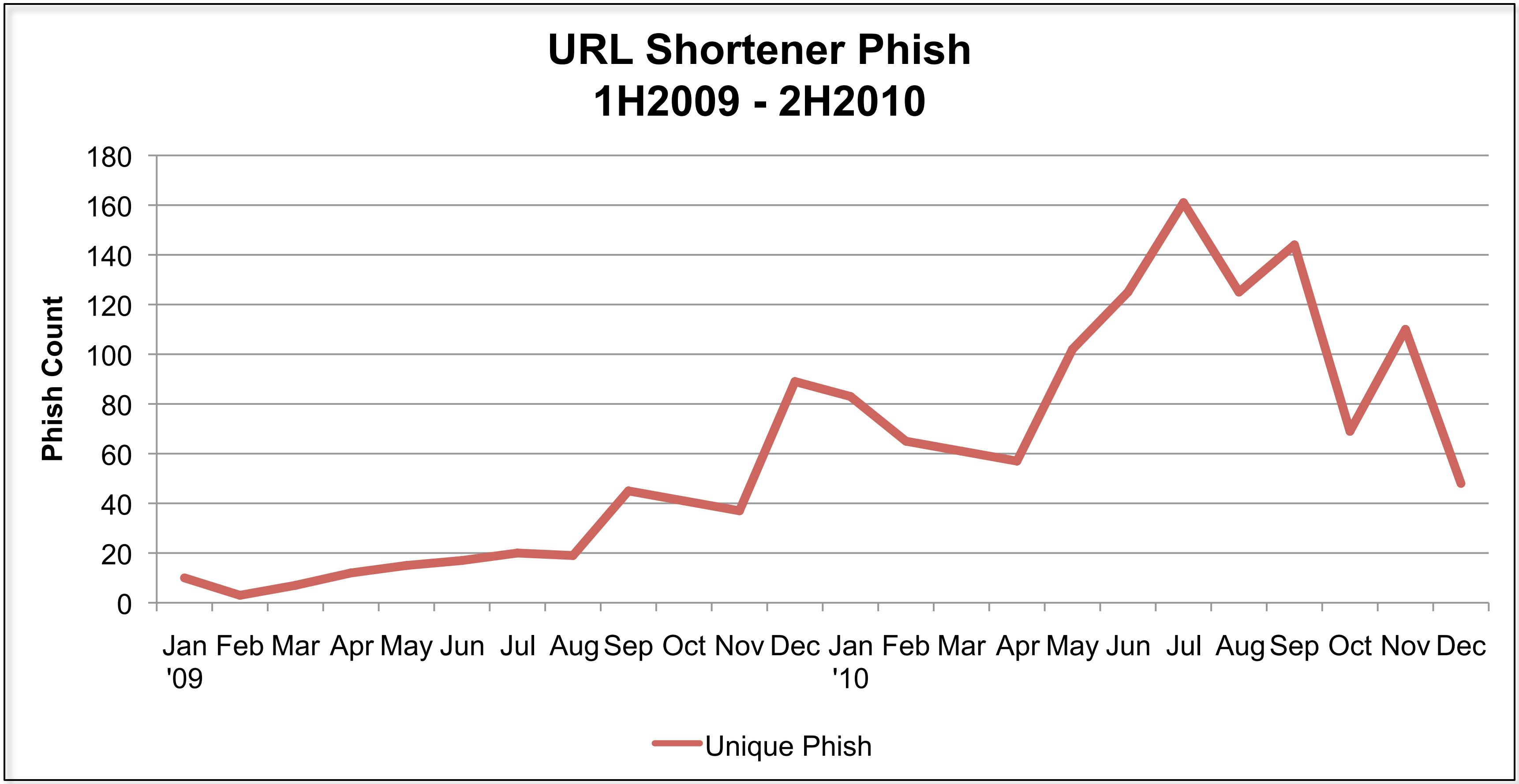
Use of Subdomain Services

- <customer_name>.<provider>.TLD
- **Use of these services by phishers almost doubled in 2H2010, to 11,768 subdomains**.
- *If we counted these unique subdomains as "regular" domain names, they would represent 22% of all domains used for phishing.*
- 40% of phishing subdomains were on **CO.CC**

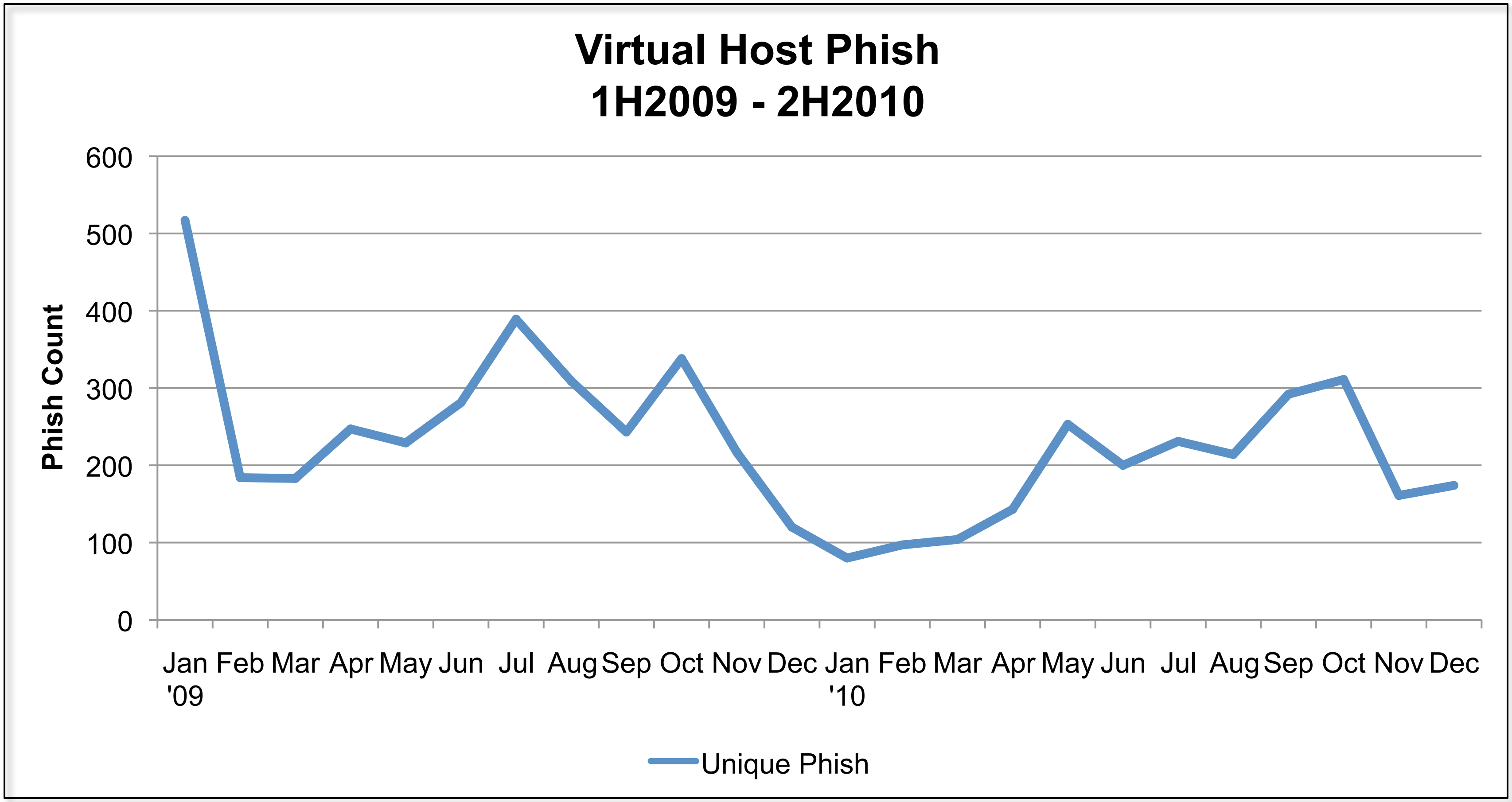
Subdomain Service Phish



URL Shorteners



Virtual Hosts



Internationalized Domain Names (IDNs)

- In last three years, we have only found two homographic attacks.
- July 12, 2010:

  http://xn--fcebook-hwa.com = http://fácebook.com

- 36 new IDN TLDs have been approved
  - Russian Federation: .РФ (.RF in Cyrillic, .xn--p1ai)

Conclusions

- Clamp down in one place and the problems simply move elsewhere.
- Free services like CO.CC and .TK are being abused heavily by phishers.
- Subdomain services are as big a problem as the registration of regular domain names.
- Uptimes got higher – watch out!

APWG Global Phishing Survey 2H2010
Thank You!

For more information or data for your TLD:

Rod Rasmussen rod.rasmussen <at> internetidentity.co

Greg Aaron gaaron <at> afilias.info