Global Phishing Survey 2H2009

Greg Aaron

Rod Rasmussen

Released May 11, 2010

http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

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 191,771,389 domain names in the TLDs we have stats for. Accounts for ~ 99.5% of domain names in the world.

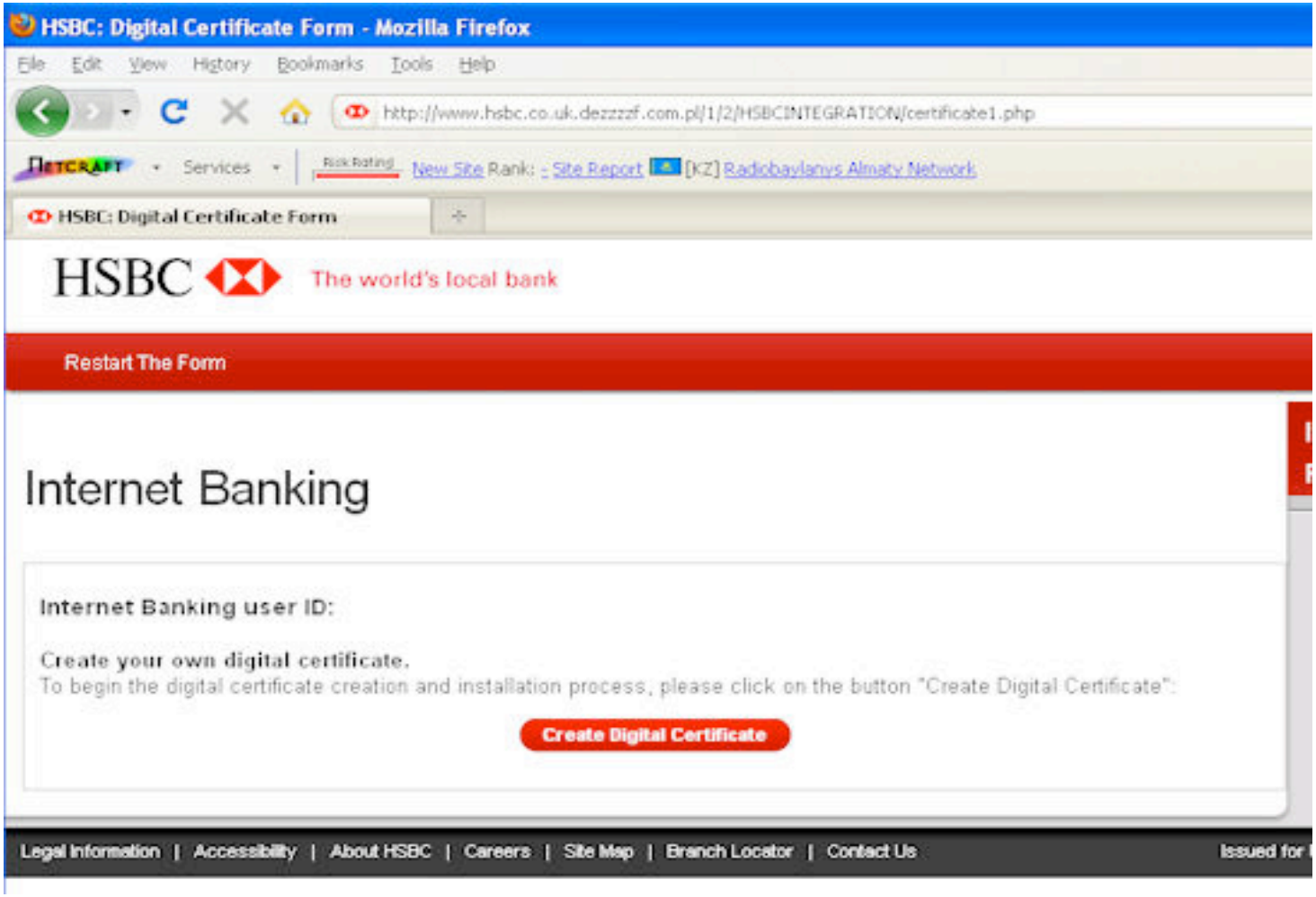
Basic Statistics

	2H2009	1H2009	2H2008	1H2008
Phishing domain names	**28,775**	30,131	30,454	26,678
Attacks	**126,697**	55,698	56,959	47,324
TLDs used	**173**	171	170	155
IP-based phish (unique IPs)	**2,031**	3,563	2,809	3,389
Maliciously registered domains	**6,372**	4,382	5,591	-
IDN domains	**12**	13	10	52

Avalanche

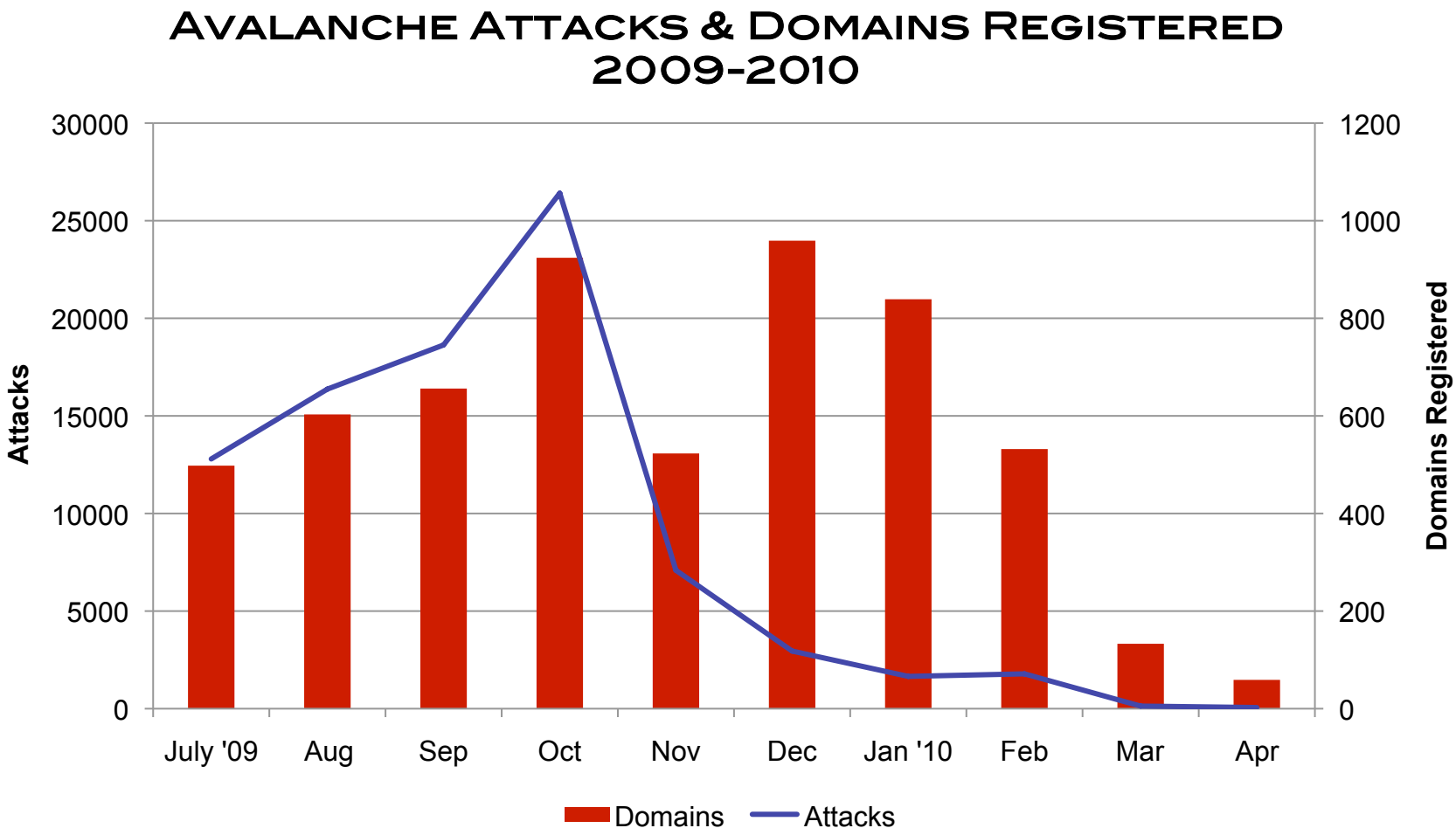
- **Avalanche responsible for two-thirds of all the phishing attacks seen during 2H2009 -- 84,250 out of 126,697.**
- Fast-flux (botnet) hosting. Mitigate by taking down the domain names.
- Used domains in 33 TLDs
- Zeus crimeware

Avalanche / Zeus



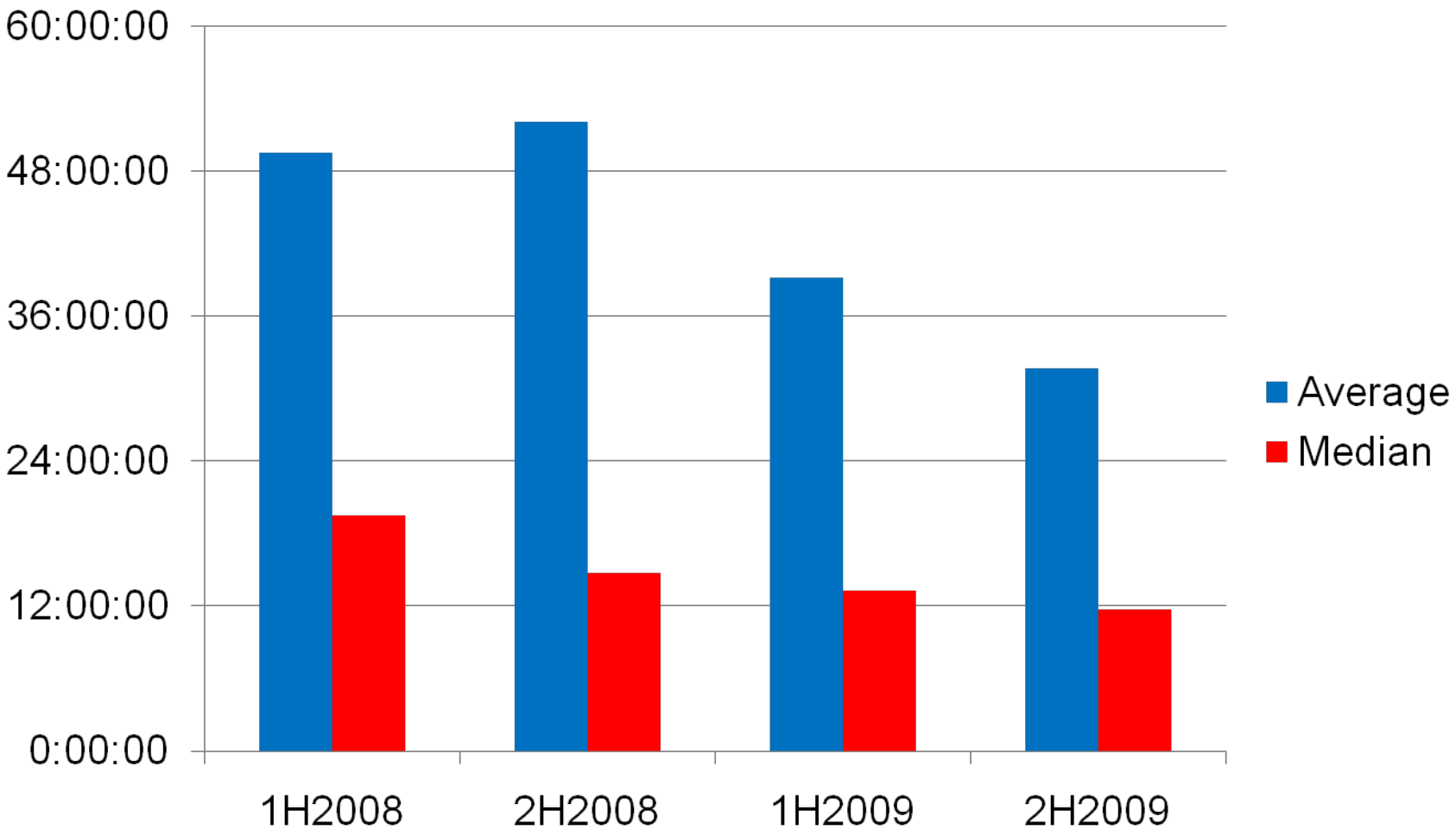
APWG Committed to Wiping Out Internet Scams and Fraud

Targeting Avalanche



APWG Committed to Wiping Out Internet Scams and Fraud

Phishing Site Uptimes (HH:MM:SS)



APWG Committed to Wiping Out Internet Scams and Fraud

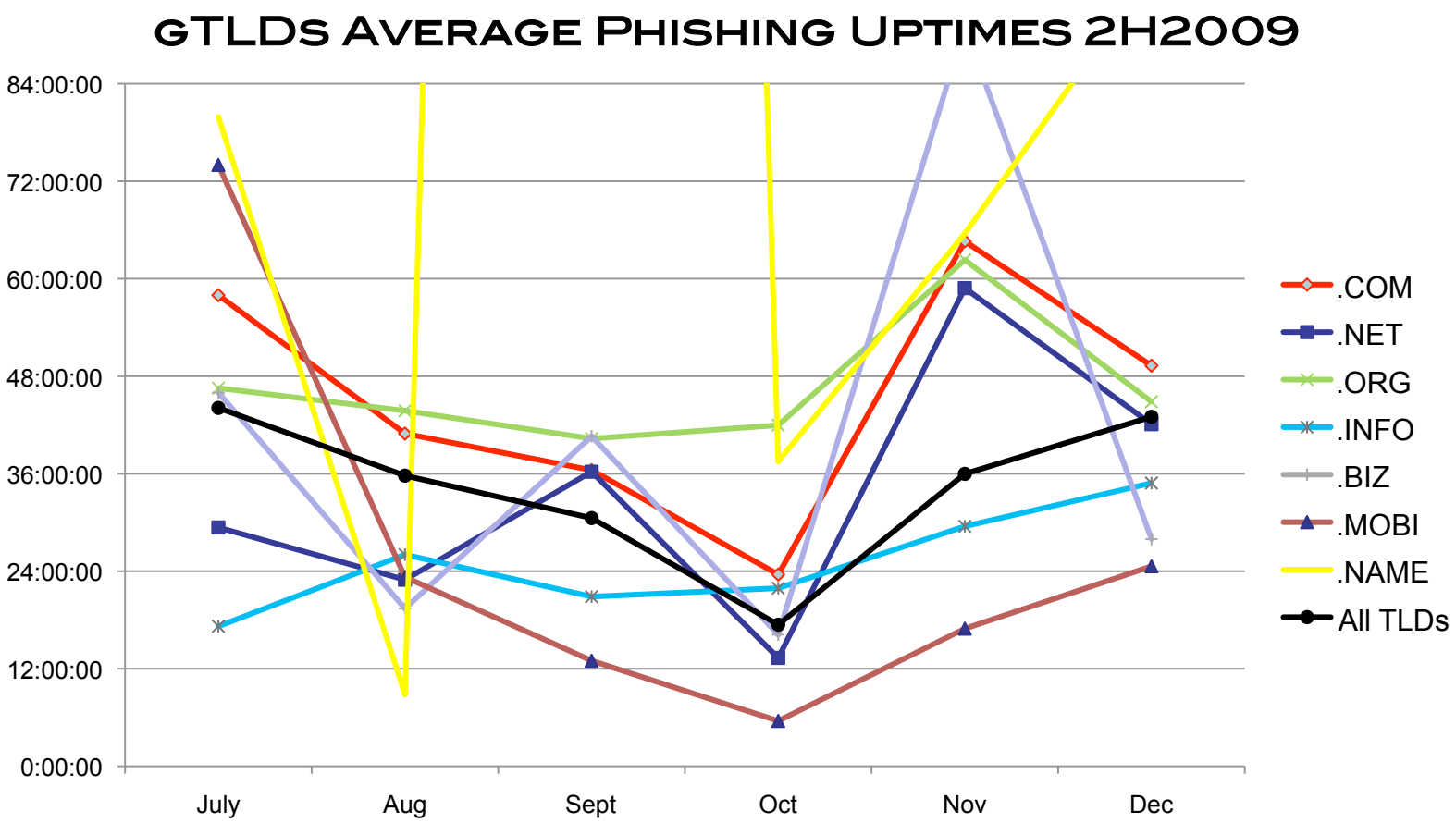
Uptimes

- The median has fallen remarkably over the past two years, from 19:30 in 1H2008 to 11:44 in 2H2009.
- Avalanche domains were killed quickly. On average, Avalanche phish lasted half as long as non-Avalanche phish.
- Non-Avalanche phish stayed up noticeably longer in 2H2009 than they did in 1H2009.

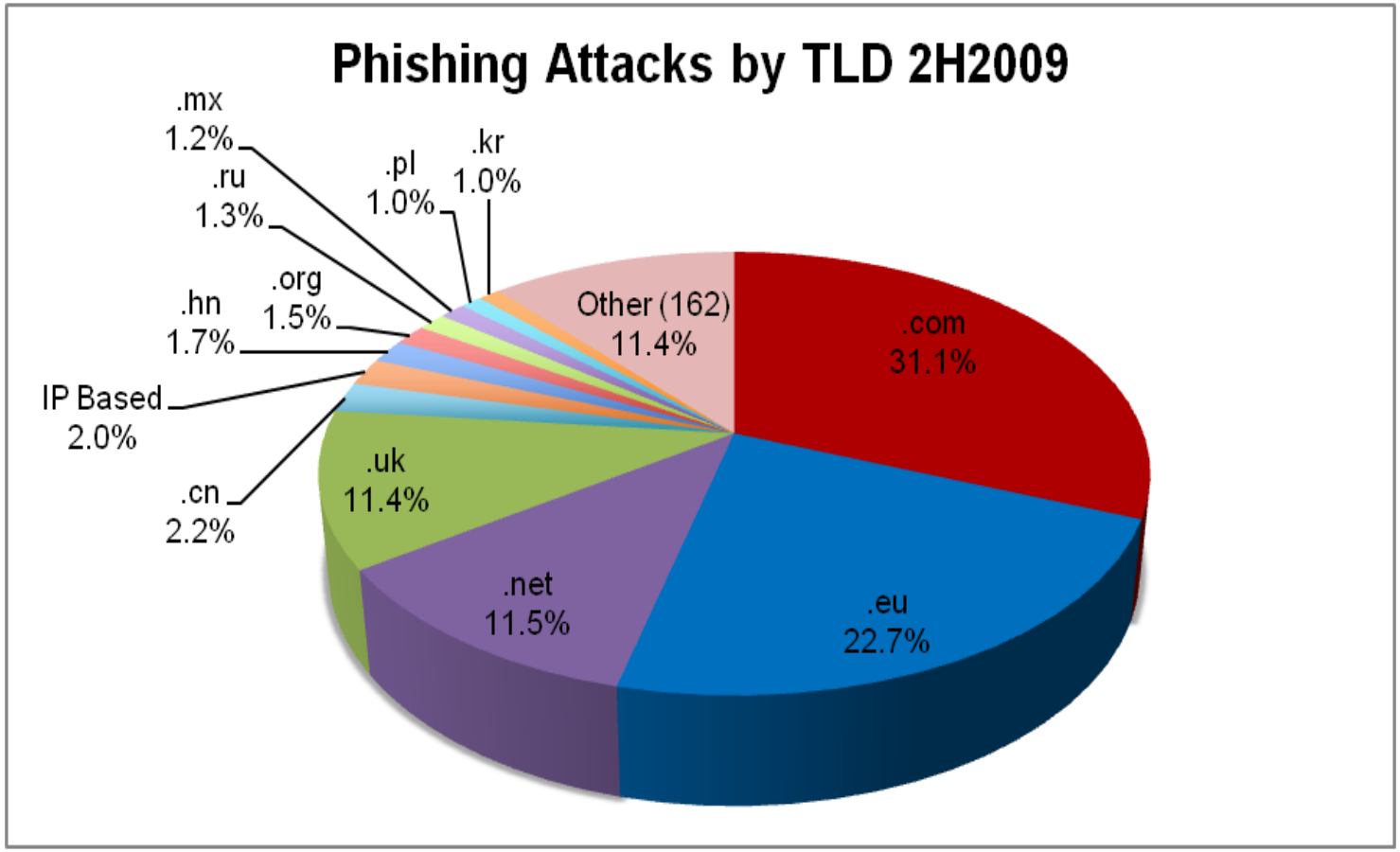
	Average (HH:MM:SS)	Median (HH:MM:SS)
All phish 2H2009	**31:38:00**	**11:44:15**
Avalanche 2H2009	**15:35:51**	**10:32:35**
Non-Avalanche 2H2009	**63:27:46**	**17:49:01**
Non-Avalanche 1H2009	**45:36:00**	**14:03:00**

Uptimes

(HH:MM:SS)

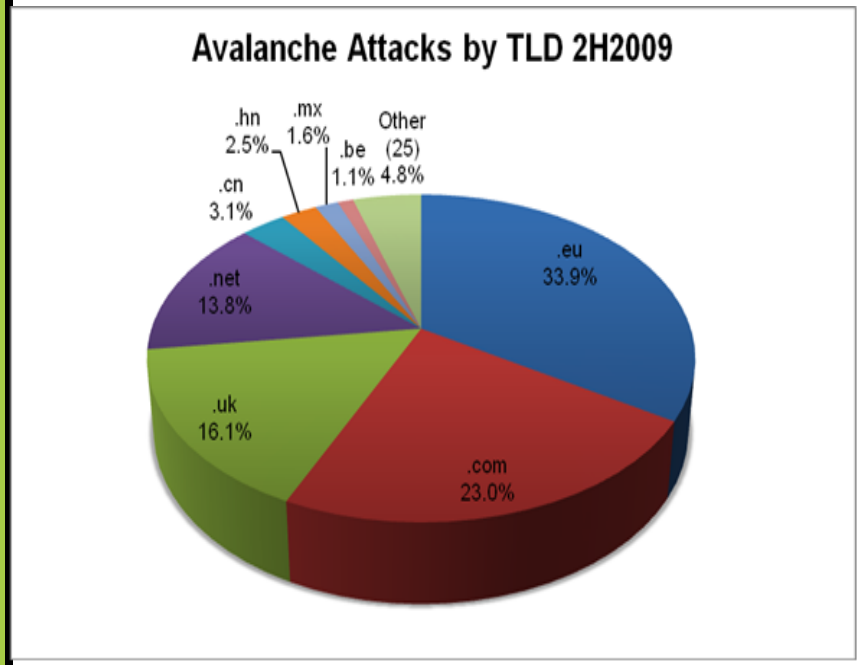


Phishing Rates by TLD

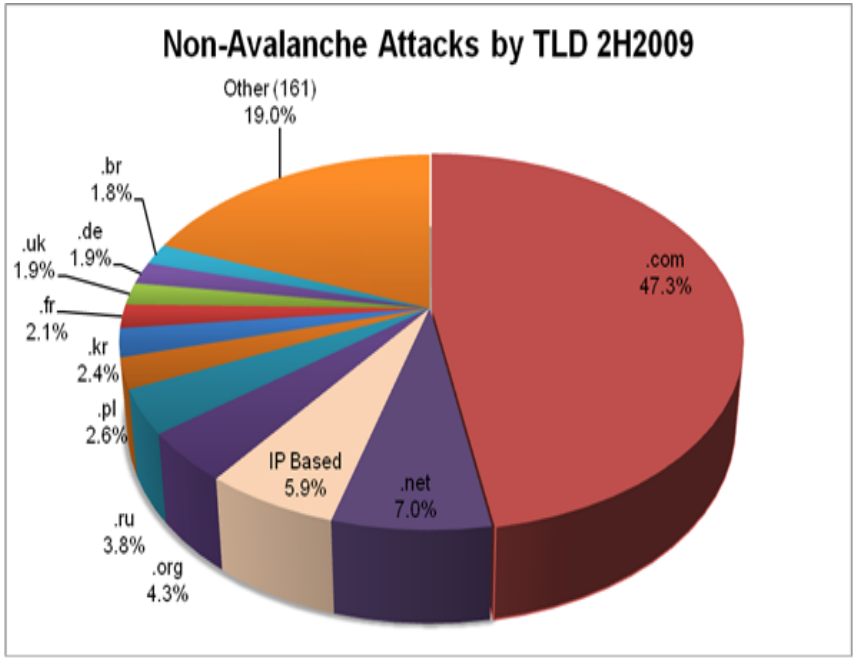


By TLD: Avalanche vs. Other

86% in .COM, .EU, .NET, .UK



Distributed more by market share



APWG Committed to Wiping Out Internet Scams and Fraud

Phishing by TLD: Score

- Metric: “Phishing Domains per 10,000”
  - Measures prevalence of phishing in a TLD
  - Median score: **2.9**
  - .COM score: **1.6**
  - Scores between 1.6 and 2.9 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)

	TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009
1	.th	Thailand	117	60	48,111	**12.5**	**24.3**
2	.kr	Korea	1,278	580	1,061,187	**5.5**	**12.0**
3	.ie	Ireland	100	65	135,177	**4.8**	**7.4**
4	.be	Belgium	1,111	444	966,679	**4.6**	**11.5**
5	.ro	Romania	295	134	325,000	**4.1**	**9.1**
6	.my	Malaysia	45	36	89,798	**4.0**	**5.0**
7	.eu	European Union	28,793	1,234	3,140,216	**3.9**	**91.7**
8	.ir	Iran	68	43	144,865	**3.0**	**4.7**
9	.pl	Poland	1,329	470	1,638,550	**2.9**	**8.1**
10	.mx	Mexico	1,466	104	376,455	**2.8**	**38.9**

Mitigation at TLDs

- .EU, .BE, .COM, .NET hit hard by Avalanche
- Nominet's .UK program
  - Outreach
  - "Phish Lock" status
- .HN (Honduras) and .IM (Isle of Man) response
- Continued success of registry-level mitigation efforts (.HK, .BIZ, .INFO, .ORG)

Malicious Registrations

- Of the 28,775 phishing domains:
  - **~78% were compromised/hacked**
  - **~22% were registered by phishers** (6,372). Most of those – 4,151 – were registered by Avalanche.
  - 1,063 domains contained a relevant brand name or brand *misspelling*. This is 17% of maliciously registered domains, and just 3.6% of all domains that were used for phishing.
- 81% of the malicious registrations were made in just 5 TLDs: .BE, .COM, .EU, .NET, and .UK

Internationalized Domain Names (IDNs)

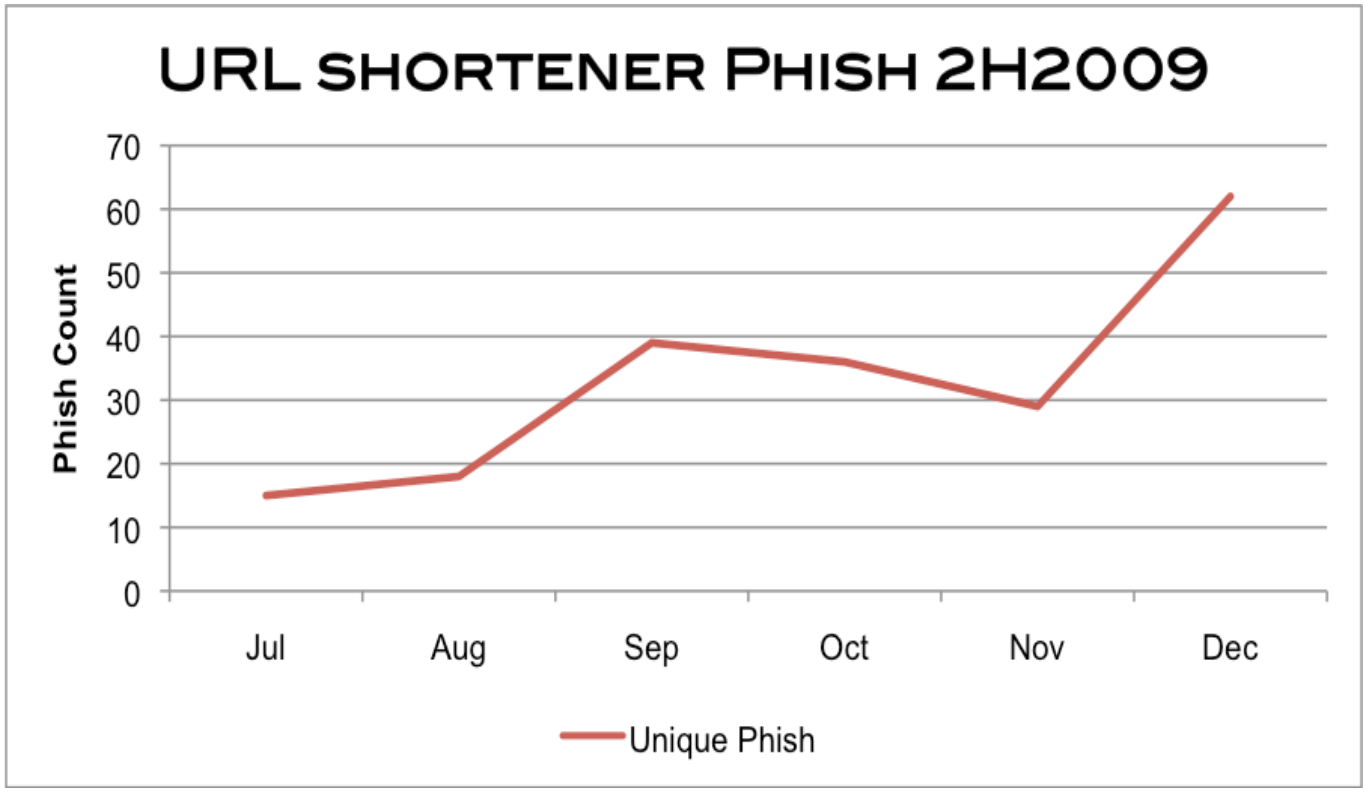
- In last two
  ye
  a
  rs, we have only found one homographic attack:

  xn--hotmal-t9a.net = hotmaıl.net
- New IDN TLDs underway
  - 21 applications in 11 languages, so far
  - *Russian Federation*: .РФ (.RF in Cyrillic, .xn--p1ai)
  - *UAE*: امارات . (Arabic .emarat, .xn--wgbh1c)
  - *China*: Three
    TLDs: .CN,
    S
    implified (.xn--g6w251d), and Traditional (.xn--fiqs8S)

Subdomain Services

- <customer_name>.<provider>.TLD
- In 2H2009, subdomain services hosted 6,734 phish (versus 6,441 in 1H2009)
- This is more than the number of domains names purchased by phishers at regular domain name registrars (6,372)
- Subdomain services account for the majority of phishing in some large TLDs.
- Changes in subdomain marketplace

URL Shorteners



Conclusions

- Avalanche dominated phishing into 2010 but has faded. *What will happen next?*
- Average and median uptimes of phishing attacks dropped.
- In general, seems that domain name registrars and registries improved response to Avalanche.

Conclusions

- Some registrars and registries continued to be vulnerable to Avalanche.
- Non-Avalanche phishing got less attention?
- IDNs not being leveraged by phishers.
- Responders should cultivate contacts at subdomain resellers.

Global Phishing Survey: 2H2009

Thank You!

Questions?

http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

rod.rasmussen<at>antiphishing.org

APWG Committed to Wiping Out Internet Scams and Fraud